Paulo Fernando da Silva

RACLOUDS – MODELO PARA ANÁLISE DE RISCO EM CLOUDS NO CONTEXTO DE ATIVOS DE INFORMAÇÕES

Tese de doutorado submetida ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina para a obtenção do Grau de Doutor em Ciência da Computação.
Orientador: Prof. Dr. Carlos Becker Westphall.

Florianópolis
2015

Ficha de identificação da obra elaborada pelo autor
através do Programa de Geração Automática da Biblioteca Universitária
da UFSC.

A ficha de identificação é elaborada pelo próprio autor
Maiores informações em:
http://portalbu.ufsc.br/ficha

Paulo Fernando da Silva

RACLOUDS – MODELO PARA ANÁLISE DE RISCO EM CLOUDS NO CONTEXTO DE ATIVOS DE INFORMAÇÕES

Esta tese foi julgada adequada para obtenção do título de doutor e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Florianópolis, 2 de dezembro de 2015.

_____
Profª. Carina Friedrich Dorneles, Drª
Coordenadora do PPGCC

Banca Examinadora:

_____
Prof. Carlos Becker Westphall, Dr.
Orientador
Universidade Federal de Santa Catarina

_____
Prof. Nelson Luis Saldanha da Fonseca, Dr.
Universidade Estadual de Campinas

_____
Prof. Bruno Richard Schulze, Dr.
Laboratório Nacional de Computação Científica

_____
Prof. Marcelo Ricardo Stemmer, Dr.
Universidade Federal de Santa Catarina

_____
Prof. Rômulo Silva de Oliveira, Dr.
Universidade Federal de Santa Catarina

_____
Profª. Silvia Modesto Nassar, Drª
Universidade Federal de Santa Catarina

_____
Prof. Mario Antonio Ribeiro Dantas, Dr.
Universidade Federal de Santa Catarina

Este trabalho é dedicado ao meu orientador Prof. Dr. Carlos Becker Westphall e aos meus queridos pais Oscar e Diná, e a minha amada esposa Viviane.

AGRADECIMENTOS

Agradeço aos meus colegas do Laboratório de Redes e Gerência e aos professores Carlos e Carla, pela inestimável colaboração no desenvolvimento deste trabalho.

O homem erudito é um descobridor de fatos que já existem – mas o homem sábio é um criador de valores que não existem e que ele faz existir.

(Albert Einstein)

RESUMO

A computação em nuvem oferece benefícios em termos de disponibilidade e custo, porém afasta a gerência de segurança da informação do cliente da nuvem, transferindo-a para o provedor de serviços em nuvem. Com isto, o cliente perde o controle sobre a segurança de suas informações e serviços. Este fator tem desmotivado a migração para a computação em nuvem entre muitos clientes em potencial. Os esforços atualmente empreendidos para segurança da informação em nuvem são em sua maioria gerenciados pelo próprio provedor de serviços em nuvem, deixando o cliente novamente à margem da gerência de segurança de suas próprias informações e serviços. A análise de risco é uma importante ferramenta de gerenciamento de segurança da informação, que permite identificar as principais vulnerabilidades, ameaças e impactos em um ambiente de tecnologia da informação. Esta tese de doutorado apresenta um modelo de análise de risco para ambientes de computação em nuvem, no qual o provedor dos serviços de nuvem não seja o único responsável por todas as etapas da análise de risco. No modelo proposto o cliente da nuvem poderá realizar análises de risco em seu provedor de nuvem de modo abrangente, aderente e independente. O modelo proposto estabelece responsabilidades compartilhadas entre três entidades: Cliente, Provedor e Laboratório de Segurança, além de propor uma linguagem para representação do risco e um modelo para correlação entre os elementos integrantes da análise de risco (ameaças, vulnerabilidades e ativos de informação). A inclusão do agente demoninado de Laboratório de Segurança oferece mais credibilidade à análise de risco, tornando os resultados mais consistentes para o cliente da nuvem. Para realização de experimentos simulados foi desenvolvido um protótipo do modelo de análise de risco proposto, validando as características de abrangência, aderência e independência desejadas na análise de risco em nuvem.

Palavras-chave: Segurança da Informação. Computação em Nuvem. Análise de Risco.

ABSTRACT

Cloud computing offers benefits in terms of availability and cost, but away from the security management of the cloud customer information, transferring it to the cloud service provider. With this, the client loses control over the security of their information and services. This factor has discouraged migration to cloud computing among many potential customers. Efforts currently undertaken to cloud information security are mostly managed by own cloud services provider, leaving the client again on the margins of safety management of their own information and services. Risk analysis is an important information security management tool that enables you to identify the main vulnerabilities, threats and impacts in an information technology environment. This doctoral thesis presents a risk analysis model for cloud computing environments in which the provider of cloud services is not solely responsible for all risk analysis stages. In the model proposed the cloud customer can perform risk analysis on your cloud provider in a comprehensive way, bonded and independent. The proposed model establishes shared responsibilities among three entities: Customer, Provider and Security Laboratory, in addition to proposing a language for risk representation and a model to correlate the risk analysis integral elements (threats, vulnerabilities and information assets). The inclusion of the Security Laboratory agent provides more credibility to the risk analysis, making the most consistent results for the cloud customer. To perform simulated experiments it developed a prototype of the proposed risk analysis model, validating the completeness of features, grip and independence desired in cloud risk analysis.

Keywords: Information Security. Cloud Computing. Risk Analysis.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

A: Ativo de Informação.
AC: Asset Category.
API: *Application Program Interface.*
CC: *Cloud Consumer.*
CSA: *Cloud Security Aliance.*
CSP: Cloud Service Provider.
CVE: Common Vulnerabilities and Exponsures.
E: Evento.
DD: Degree of Deficiency.
DE: Degree of Exposure.
DI: Degree of Impact.
DMTF: *Distributed Management Task Force.*
DR: Degree of Risk.
DXP: *Dynamic eXchange Point.*
E: Evento.
IaaS: *Infrastruture as a Service.*
ISL: Information Security Labs; Information Security Laboratory.
NIST: *National Institute of Standards and Technology.*
NVD: National Vulnerability Database.
OVF: *Open Virtualization Format.*
P: Probabilidade.
PaaS: *Platform as a Service.*
pf: Probability Function.
R: Risco.
RACloud: *Risk Analisys for Clouds.*
RAP: Risk Analysis Provider.
RC: Resource Category.
RDL: Risk Definition Language.
rf: Risk Function.
RL: Risk Level.
SaaS: *Software as a Service.*
SGSI: *Sistema de Gestão de Segurança da Informação.*
SLA: Service Level Agreement.
WSRA: Web Service Risk Analysis.
XSD: XML Schema.

SUMÁRIO

1 INTRODUÇÃO

Este capítulo apresenta a contextualização do problema a ser considerado, bem como os objetivos geral e específicos. Ao final do capítulo é apresentada a seção de organização desta tese de doutorado.

1.1 CONTEXTUALIZAÇÃO DO PROBLEMA

Computação em Nuvem (*Cloud Computing*) é um paradigma que fornece a possibilidade de acesso a aplicativos e infraestrutura de software e hardware como serviço. A estrutura de cloud é fornecida aos *Cloud Consumers* (CC) por um *Cloud Service Provider* (CSP), apresentando modelos de serviço, tais como: Software como Serviço (SaaS), Plataforma como Serviço (PaaS) ou Infraestrutura como Serviço (IaaS) (MELL e GRANCE, 2011).

O paradigma de computação em nuvem tem alterado o ambiente de tecnologia da informação de empresas e instituições, que migram de um ambiente isolado com apenas poucos servidores e aplicações para ambientes integrados com grande quantidade de servidores e grande variedade de aplicações. Esta nova realidade de tecnologia da informação implica em grandes desafios de segurança para os CSPs e certa desconfiança para os CCs (SRINIVASAN 2012).

Ren (2012) afirma que questões relacionadas à segurança da informação são os primeiros obstáculos observados por clientes de nuvem para a migração de suas informações e serviços para tal ambiente. Os obstáculos de segurança existem porque o CSP está separado administrativamente do CC, que perde o controle sobre a segurança de suas informações e serviços. Mesmo que a estrutura de segurança dos CSPs seja superior à estrutura previamente encontrada nos CCs, ainda assim existe a desconfiança quanto a ameaças e vulnerabilidades internas e externas no ambiente do CSP.

A desconfiança por parte dos CCs em relação à adoção ou não de um CSP fundamenta-se no fato de que os CCs desconhecem os requisitos de segurança fornecidos pelos CSPs e desconhecem também o modo de operação dos CSPs sobre estes requisitos, ou seja, o CC desconhece o nível de maturidade dos requisitos de segurança da informação fornecidos pelo CSP. Sem fornecer meios para demonstrar a segurança do CSP para o CC, este não estará disposto a migrar suas informações e serviços para a cloud (REN, 2012).

Também a Cloud Security Alliance (2011) destaca que um dos grandes desafios para os clientes de nuvem é encontrar um modo de

avaliação de seus provedores de nuvem a fim de obter um serviço de baixo custo sem perder as características de segurança e proteção de suas informações e serviços.

A adoção de um serviço de nuvem gera para os CCs um desafio enorme, pois a menos que os provedores de nuvem possam divulgar facilmente seus controles de segurança e o alcance da implementação dos mesmos para o cliente, e o cliente saiba quais controles são necessários para manter a segurança de suas informações, existe um enorme potencial para decisões equivocadas e resultados negativos (CLOUD SECURITY ALLIANCE, 2011).

A identificação da necessidade de requisitos de segurança da informação e a análise da eficiência da implementação destes requisitos é realizada através de uma análise de risco de segurança da informação (ISO 27005, 2011). A análise de risco consiste na identificação de ameaças e vulnerabilidades que podem gerar incidentes, e na avaliação do impacto que estes incidentes podem causar sobre ativos de informação (ex. hardwares, softwares, informações, serviços, etc).

A aplicação de uma análise de risco de segurança da informação em um ambiente de computação em nuvem pode auxiliar o CC na tomada de decisão quanto à adoção ou não de um serviço de nuvem, reduzindo o potencial de decisões equivocadas e resultados negativos citados pela Cloud Security Alliance (2011). Porém, tal análise de risco deve:

- Considerar os requisitos de negócio do cliente, ou seja, ser **aderente** ao negócio e necessidades de segurança da informação do cliente;
- Considerar um amplo escopo de riscos a serem analisados, e não apenas um conjunto limitado de riscos e/ou aqueles já mitigados pelo CSP, ou seja, ser **abrangente** em relação aos requisitos de segurança analisados;
- Considerar certo grau de independência entre a entidade que terá seu risco analisado e a entidade que gerencia a análise de risco, ou seja, o resultado da análise de risco deve ser **independente** da vontade ou desejo do CSP.

Modelos de análise de risco para computação em nuvem que não observam as características de aderência, abrangência e independência dos resultados podem não gerar resultados adequados para a tomada de decisão do cliente, pois podem não levar em conta as necessidades de segurança do cliente (aderência), não contemplar a análise de requisitos

importantes de segurança da informação (abrangência) ou serem tendenciosos aos interesses do CSP (independência dos resultados).

Por outro lado, um modelo de análise de risco para computação em nuvem que atende às características de aderência, abrangência e independência dos resultados pode reduzir o potencial de decisões equivocadas por parte do cliente e os efeitos negativos advindos de tais decisões, contribuindo assim para uma adoção mais adequada de serviços de nuvem e para a disseminação da computação em nuvem.

Este trabalho de tese busca contribuir com a segurança da computação em nuvem e a evolução dos modelos de análise de risco de segurança da informação no sentido propor um modelo aderente, abrangente e independente para análise de risco em ambientes de computação em nuvem. Durante o desenvolvimento deste trabalho serão propostas as entidades participantes da análise de risco, entre elas, este trabalho contribui com a proposição da entidade ISL (Information Security Laboratory). Outras contribuições deste trabalho ocorrem no sentido de propor os componentes e fluxo de comunicação para uma análise de risco em nuvem, e propor uma linguagem para definição de risco.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O objetivo geral deste trabalho é a proposição de um modelo para análise de risco em clouds no contexto de ativos de informação. Neste modelo um cliente de nuvem pode realizar uma análise de risco de segurança da informação em um provedor de serviços de nuvem, no contexto de ativos de informação, de modo **aderente** às necessidades de segurança do cliente, **abrangente** em relação aos requisitos de segurança analisados, e com resultados **independentes** dos interesses do provedor de nuvem.

1.2.2 Objetivos Específicos

Os objetivos específicos deste trabalho são:

- Definir as diferentes entidades envolvidas em uma análise de risco para computação em nuvem e suas respectivas responsabilidades;

- Propor uma linguagem para especificação de risco e suas variáveis integrantes, como: ameaças, vulnerabilidades, ativos de informação, probabilidades e impactos;
- Propor um modelo para correlação entre ameaças, vulnerabilidades e ativos de informação em nuvem;
- Realizar a validação do modelo proposto.

1.3 ORGANIZAÇÃO DO TRABALHO

O primeiro capítulo apresenta a contextualização do problema, bem como os objetivos geral e específicos e a organização do trabalho. O segundo capítulo apresenta o estado da arte relacionado com o tema escolhido, abordando: a computação em nuvem, a segurança em nuvem, a análise de risco de segurança da informação e os trabalhos relacionados. O terceiro capítulo apresenta a abordagem da solução proposta, incluindo: a contextualização do modelo proposto, a descrição da linguagem de definição de risco e o detalhamento dos componentes do modelo proposto e sua arquitetura. O quarto capítulo apresenta o protótipo desenvolvido a partir da especificação do modelo proposto, este protótipo permite o desenvolvimento de experimentos simulados sobre o modelo proposto, os quais são apresentados no capítulo cinco. Os capítulos seis e sete contemplam os resultados e discussão e as conclusões do trabalho, respectivamente.

2 CONCEITOS, DEFINIÇÕES E ESTADO DA ARTE

Este capítulo apresenta o estado da arte relacionado com o tema desta tese. A primeira seção trata dos conceitos relacionados com a computação em nuvem. A segunda seção aborda os desafios da segurança na computação em nuvem. A terceira seção trata dos conceitos e fundamentos de análise de risco. Por fim, a quarta seção apresenta os trabalhos relacionados e uma discussão destes trabalhos em relação à solução proposta nesta tese.

2.1 COMPUTAÇÃO EM NUVEM

O NIST – *National Institute of Standards and Technology* conceitua computação em nuvem como um modelo de fornecimento para acesso à rede sob demanda com compartilhamento de recursos computacionais configuráveis, que podem ser rapidamente alocados e liberados com o mínimo de interação com o provedor (MELL e GRANCE, 2011).

Os conceitos relativos à computação em nuvem definidos pelo NIST foram visualmente organizados pela CSA – *Cloud Security Aliance* na Figura 1 (CLOUD SECURITY ALLIANCE, 2011).

Um ambiente de nuvem computacional é composto por cinco características essenciais: amplo acesso à rede, rápida elasticidade, serviços mensuráveis, auto-serviço sob demanda e pool de recursos.

O amplo acesso à rede permite o acesso aos serviços de cloud através de uma grande quantidade de dispositivos heterogêneos, como smartphones e/ou tablets.

A rápida elasticidade garante que recursos podem ser rapidamente e facilmente alocados para determinado cliente conforme sua necessidade, e após o uso estes recursos também serão rapidamente e facilmente desalocados.

A característica de serviços mensuráveis trata da contabilização dos recursos fornecidos pelo provedor e utilizados pelo cliente, ou seja, em um ambiente de computação em nuvem deve ser possível mensurar os níveis de recursos utilizados. Esta característica pode ser útil para a cobrança dos serviços do provedor junto ao cliente e do cliente junto ao provedor.

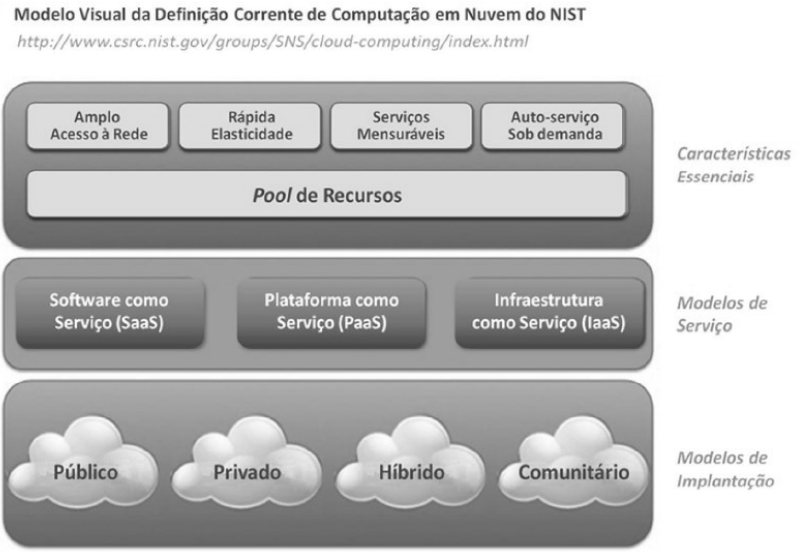
O auto-serviço sob demanda permite ao cliente provisionar recursos sem interação com o provedor de serviços. O provisionamento de recursos podem incluir, por exemplo, a reserva de tempo de

processamento junto ao servidor ou a alocação de espaço de armazenamento na cloud.

O pool de recursos consiste no conjunto de recursos fornecidos pelo provedor ao cliente de nuvem. Estes recursos possuem características de interdependência física e multilocação que muitas vezes não são visíveis ou acessíveis ao cliente, pois os recursos são compartilhados entre os clientes em um nível mais baixo de abstração no ambiente de nuvem.

Outra característica muito discutida na computação em nuvem é a virtualização. Esta não é uma característica essencial, ou seja, não é um requisito existir a virtualização para se ter um ambiente de nuvem. Entretanto muitos ambientes de nuvem são estruturados sobre ambientes virtuais, pois a construção de máquinas virtuais contribui em muito para o atendimento de requisitos essenciais como a rápida elasticidade ou o amplo acesso à rede.

Figura 1 – Conceitos de Cloud Computing.



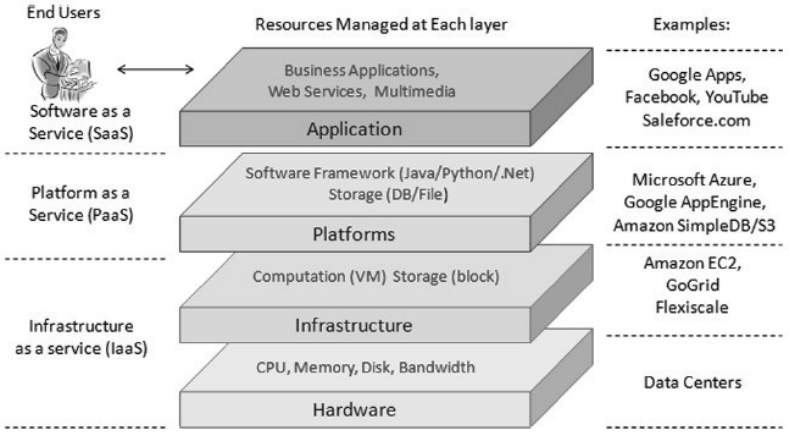
Fonte: Cloud Security Aliance (2011).

Outras características normalmente associadas a ambientes de computação em nuvem são: pagamento apenas pelo serviço utilizado, grande facilidade de uso, alta disponibilidade, baixo investimento inicial e baixo custo de operação para o cliente da cloud.

Os modelos de serviço de um ambiente de nuvem podem ser organizados em três níveis: Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) ou Software como Serviço (SaaS).

Em conformidade com os modelos de serviço definidos pelo NIST, Höfer e Karagiannis (2011) descrevem uma arquitetura de computação em nuvem dividida em quatro camadas: hardware, infraestrutura, plataforma e aplicação. Nesta arquitetura os serviços oferecidos pela cloud podem estar organizados de três maneiras diferentes, conforme Figura 2.

Figura 2 – Modelos de Serviço de Computação em nuvem.



Fonte: Höfer e Karagiannis (2011).

A primeira forma de organização dos serviços de computação em nuvem, IaaS – Infraestutura como Serviço, consiste no fornecimento apenas de virtualização de recursos de armazenamento e processamento. Uma característica importante desta forma de serviço é a associação dinâmica de recursos físicos compartilhados entre diferentes clientes. Exemplos deste tipo de serviços são a Amazon EC2, GoGrid e GigaSpaces.

A segunda forma de organização dos serviços de computação em nuvem, PaaS – Plataforma como Serviço, fornece aos clientes mais do que infraestrutura, nesta organização já estão disponíveis sistemas operacionais e aplicações básicas como: Java, phyton, .net, entre outras. Exemplos deste tipo de organização são: MS-Azure, Google AppEngine e Amazon SimpleDB.

Ainda segundo a arquitetura de Höfer e Karagiannis (2011), a terceira forma de organização dos serviços de computação em nuvem é a SaaS – Software como Serviço. Nesta organização é fornecida ao cliente uma estrutura completa com hardware, infraestrutura, plataforma e aplicações. Exemplos desta organização são o Google docs, o CRM Saleforce.com e o Facebook.

O último conjunto de conceitos definidos pelo NIST para computação em nuvem trata dos modelos de implantação (Figura 1), que podem ser organizados em público, privado, híbrido ou comunitário.

A nuvem pública consiste em uma estrutura de nuvem de um provedor que a fornece (vende) ao público em geral (clientes). Já a nuvem privada ocorre quando a estrutura de nuvem é consumida por uma única organização. Esta organização pode também administrar sua nuvem privada ou pode delegar a administração para terceiros. A nuvem privada pode estar localizada dentro ou fora da organização que a consome.

Uma nuvem comunitária ocorre quando entidades com fins correlatos se associam para a construção de um ambiente de nuvem. A nuvem comunitária será consumida pelo conjunto das entidades que a construiu e poderá ser administrada pelo conjunto das entidades ou por terceiros. Da mesma forma como ocorre na nuvem privada, a nuvem pública pode estar localizada dentro ou fora da organização. Por fim, no modelo de implantação de nuvem híbrida tem-se características mistas de pelo menos dois modelos previamente citados.

Vários artigos têm discutido diferentes aspectos da computação em nuvem nos últimos anos. Dey (2013) discute a integração de dispositivos móveis com ambientes de computação em nuvem, destacando que a computação em nuvem pode suprir as limitações de bateria e processamento dos dispositivos móveis. O uso de computação em nuvem para dispositivos móveis pode permitir o desenvolvimento de aplicações mais robustas para estes dispositivos, porém nestes casos a conectividade é um fator importante a ser considerado.

Iosup et al. (2012) comentam a apresentação e demonstração de resultados sobre o uso da computação em nuvem, especificamente a IaaS, ainda é um fator limitante da adoção de soluções de cloud. O autor discute uma abordagem quantitativa para avaliação de provedores de IaaS, que combina análises empíricas com modelagem e simulação de casos de uso do IaaS.

Zhou et at. (2013) apresentam os desafios da realização de testes de desempenho em ambientes de computação em nuvem. São discutidos alguns fatores de desempenho específicos de computação em nuvem e

agravantes na obtenção de avaliações de desempenho adequadas, como: a grande variação de performance entre as plataforma de cloud e problemas relacionados à segurança.

Kolluru (2013) discute o problema e soluções relacionadas com a conexão das aplicações do cliente de nuvem ao ambiente de nuvem. São discutidas questões como a integração de diferentes serviços e aplicações, o uso de diferentes dispositivos (mobilidade), a performance e usabilidade das aplicações em cloud, além do uso da cloud em conjunto com aplicações legadas.

Lor et al. (2012) apresentam os problemas envolvidos na implantação de aplicações em ambientes de computação em nuvem federados, onde o isolamento fim-a-fim, a escalabilidade e a qualidade de serviço são fatores críticos. O artigo descreve um modelo para colaboração entre os componentes da federação em nuvem, usando o conceito de *Dynamic eXchange Point* (DXP) para realizar conexões entre pontos de diferentes domínios.

2.2 SEGURANÇA EM NUVEM

Embora a computação em nuvem possa fornecer redução de custo e alta escalabilidade e disponibilidade para as empresas, um grande desafio é a garantia da conformidade com requisitos de segurança para as informações e serviços alocados na nuvem (SONG, 2012).

Um ambiente de nuvem computacional necessita de todos os controles de segurança da informação necessários a outros ambientes de tecnologia da informação tradicionais. Porém, a arquitetura, as tecnologias e os modelos operacionais aplicados na computação em nuvem podem introduzir novos riscos se comparados aos modelos de tecnologia da informação tradicionais, consequentemente gerando a necessidade de diferentes controles de segurança da informação (CLOUD SECURITY ALIANCE, 2011).

Vários artigos comentam os desafios de segurança da informação na computação em nuvem (MORIN, 2012) (YU, 2012) (SRINIVASAN 2012) (ALFATH, 2013) (ROT, 2013). Entre os principais desafios citados estão:

- **Privacidade dos dados de usuários**: consiste em garantir que os dados dos usuários não sejam vistos por entidades não autorizadas. Este desafio é potencializado em um ambiente

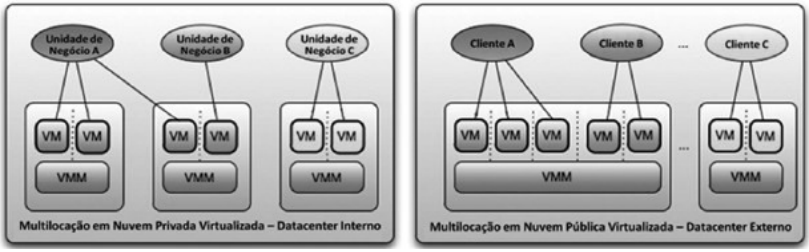
compartilhado entre diferentes clientes, como ocorre em ambientes de computação em nuvem;

- **Ameaças externas**: consiste em ataques como man-in-the-middle, packet sniffing, IP spoofing e denial of service, que ocorrem fora do ambiente de computação em nuvem. Este desafio é agravado em ambientes de cloud, onde o CC acessa os recursos do CSP através de uma rede pública, como a internet;
- **Ameaças internas**: no ambiente de computação em nuvem o CC perde o controle direto de sua infraestrutura de tecnologia da informação, que é controlada pelos funcionários do CSP. Isto torna o ambiente vulnerável a ameaças internas ao CSP, como a publicação indevida de dados de usuários por parte de um funcionário do CSP;
- **Interfaces de aplicação inseguras**: ocorre quando o CSP fornece interfaces mal projetadas ou mal configuradas para o CC. Neste caso um agente mal intencionado pode fazer uso das interfaces inseguras para acessar dados não autorizados ou realizar operações indevidas;
- **Gerenciamento de identidades**: consiste na garantia da identidade de um usuário e dos recursos que este usuário pode acessar. A caraterística de grande elasticidade e pagamento pelo uso torna o gerenciamento de identidades de ambientes de computação em nuvem altamente complexo e potencialmente vulnerável;
- **Gerenciamento da virtualização**: virtualização é uma questão chave para o funcionamento dos ambientes de *computação em nuvem*. A virtualização em grande escala pode gerar importantes vulnerabilidades, como por exemplo, a perda da separação física entre as diferentes máquinas virtuais de um ambiente de nuvem;
- **Gerenciamento de chaves criptográficas**: embora o gerenciamento de chaves seja um fator crítico em todos os ambientes computacionais, este fator pode ser potencializado nos ambientes de *computação em nuvem* devido ao fato de que os atuais mecanismos de criptografia não são totalmente aderentes aos requisitos de canal de comunicação, armazenamento, atualização, virtualização, mapeamento e isolamento dos ambientes de computação em nuvem;

- **Conformidade com normas e regulamentos**: a governança dos dados e a conformidade com normas de segurança é um requisito crítico para os CSP, seja para garantir a confiança de seus clientes ou para o atendimento a requisitos legais e de relacionamento com o governo. Algumas normas que devem ser observadas pelos CSPs são: SOX, HIPAA, FISMA, FIPS 140-2, GLBA, ITAR, ISAE 3402, ISO/IEC 27001, SAS 70 e SSAE 16;
- **Gerenciamento de SLAs**: SLAs (Service Level Agreement) são estabelecidos entre CSP e CC para definir o nível de serviços respectivamente fornecido\aceito. Vulnerabilidades podem ser inseridas neste contexto quando o CC não conhece ou entende os requisitos de segurança que devem fazer parte do SLA.

Para Cloud Security Alliance (2011) a característica de multilocação da computação em nuvem é um fator relevante na gestão da segurança da informação. Conforme apresenta a Figura 3, a multilocação consiste no compartilhamento de recursos da cloud entre diferentes unidades de negócio (modelo de cloud privada) ou mesmo entre clientes de diferentes empresas (modelo de cloud pública).

Figura 3 – Multilocação na computação em nuvem.



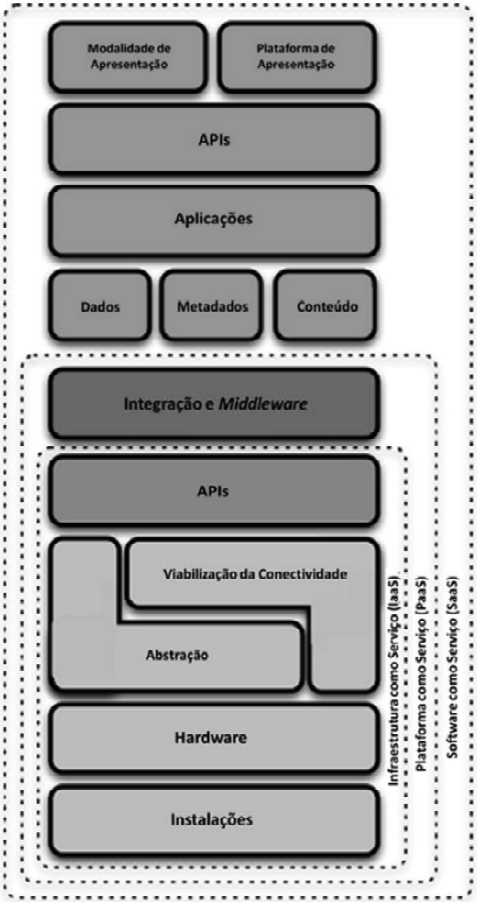
Fonte: Cloud Security Aliance (2011).

A multilocação gera a necessidade de controles de segurança da informação específicos para o gerenciamento do compartilhamento dos recursos. Tais controles envolvem o desenvolvimento de políticas específicas, bem como controles de segmentação e isolamento lógico, com o objetivo de garantir a confidencialidade, integridade e disponibilidade dos diferentes clientes.

Os modelos de serviço (IaaS, PaaS e SaaS) da computação em nuvem também influenciam diretamente no gerenciamento da segurança da informação. A Figura 4 apresenta um modelo de referência de

computação em nuvem discutido por Cloud Security Alliance (2011). Neste modelo é possível identificar as diferentes camadas de serviços oferecidos pelos modelos IaaS, PaaS e SaaS.

Figura 4 – Modelo de referência de nuvem.



Fonte: Cloud Security Aliance (2011).

Os níveis de serviço estão diretamente relacionados com a segurança da informação no sentido de que cada nível de serviço apresenta diferentes responsabilidades de segurança da informação para o CSP e CC. No nível de serviço IaaS o CSP é responsável somente pela segurança da informação associada à infraestrutura, como instalações, hardware e virtualização. Neste nível questões de segurança

relacionadas com a plataforma e a aplicação continuam sendo responsabilidade do cliente.

Caso o cliente contrate um nível de cloud de PaaS, o CSP passa também a responder pela segurança da informação do nível de plataforma, ou seja, a segurança da camada de integração e middleware (Figura 4) passa a ser responsabilidade do CSP, e o CC fica apenas com a responsabilidade da segurança da informação do nível de software.

Um CSP que entrega a seu cliente um modelo de serviço SaaS é responsável pela segurança da informação em todos os níveis da arquitetura da computação em nuvem. Neste caso o CSP fica responsável pela segurança desde a infraestrutura até ao nível de software, incluindo os dados, as aplicações e as APIs de acesso (Figura 4). Neste modelo o cliente não possui responsabilidades pela segurança dos recursos oferecidos nos níveis de infraestrutura, plataforma ou software.

Observa-se então que quanto mais baixo for o nível de serviço contratado pelo CC, maior será a sua responsabilidade em relação à segurança da informação na nuvem, pois o CSP não terá responsabilidade pelos níveis não contratados e consequentemente gerenciados diretamente pelo CC. Este entendimento é essencial na discussão de qualquer aspecto de segurança da informação relacionado com a computação em nuvem (CLOUD SECURITY ALLIANCE, 2011).

Além dos modelos de serviço, os modelos de implantação (público, privado, híbrido e comunitário) também influenciam diretamente na gestão de segurança da informação da computação em nuvem. Os modelos de implantação são geralmente analisados sob o aspecto de localização física interna ou externa, onde geralmente o modelo público denota uma localização interna e o modelo privado denota uma localização externa.

Porém para a segurança da informação existem outros aspectos relevantes nos modelos de implantação além da localização geográfica. Questões como quem é o proprietário, quem gerencia a infraestrutura e quem são os clientes que acessam a cloud também são relevantes. A Figura 5 relaciona estas questões com os modelos de implantação em nuvem.

Figura 5 – Modelos de implantação de nuvem.

Fonte: Cloud Security Aliance (2011).

Conforme a Figura 5, uma implantação pública é de propriedade e gerenciamento terceirizado, e localização externa. Já uma implantação privada ou comunitária pode ter qualquer combinação de responsabilidade (organização ou terceiro) relacionada com a propriedade e gerenciamento da infraestrutura, além de poder estar localizada dentro ou fora da organização. Uma implantação híbrida combina todas as opções de gerenciamento, propriedade e localização, conforme participação de cada entidade no modelo híbrido.

A última coluna da Figura 5 indica quem são os consumidores (usuários) da cloud em questão. São considerados consumidores confiáveis àqueles submetidos à política de segurança da informação ou normas e regulamentos próprios internos da organização. Consumidores não confiáveis acessam a cloud sem estarem sujeitos à política de segurança da informação ou regulamentos internos da organização.

As questões acima discutidas relacionadas com os modelos de implantação em nuvem são relevantes para a segurança da informação, pois definem as possíveis entidades responsáveis pela gestão de segurança da informação em cada modelo de implantação.

2.3 ANÁLISE DE RISCO EM SEGURANÇA DA INFORMAÇÃO

A série de normas ISO 27000 estabelece requisitos para estabelecer, implementar, manter, melhorar continuamente um sistema

de gestão de segurança da informação (ISO 27001, 2013). As principais normas da série ISO 27000 são:

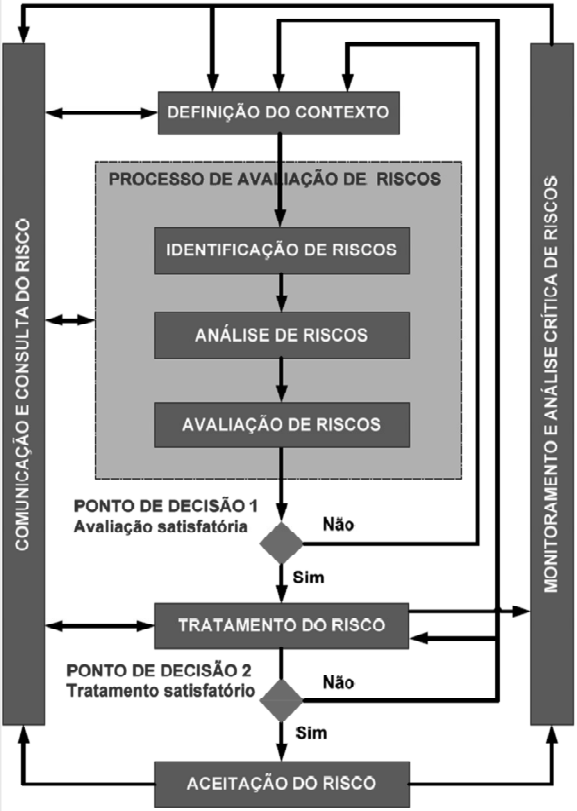
- ISO 27000 – apresenta uma visão geral das normas e vocabulário;
- ISO 27001 – define os requisitos no estabelecimento do sistema de gestão de segurança da informação (SGSI);
- ISO 27002 – apresenta um conjunto de controles e objetivos de controle de segurança da informação;
- ISO 27003 – apresenta linhas gerais para a implementação do SGSI;
- ISO 27004 – define linhas gerais para a criação de métricas de segurança da informação e a medição do sistema de gestão de segurança da informação;
- ISO 27005 – fornece diretrizes para o processo de gestão de risco em segurança da informação;
- ISO 27006 – apresenta recomendações para o processo de auditoria e certificação em segurança da informação.

A ISO 2005 (2011) define risco como sendo o efeito da incerteza sobre os objetivos de controle de segurança da informação. O risco também pode ser definido como a combinação das consequências advindas da ocorrência de um evento indesejado com a probabilidade da ocorrência deste evento. Já a análise de risco consiste no processo de compreender a natureza do risco e determinar o nível de risco de determinado evento. O nível de risco fornece uma medida da magnitude do risco, calculada em termos da consequência da realização do risco e da probabilidade da ocorrência do risco.

A análise de risco fornece elementos para a realização da avaliação de risco. Avaliação de risco, segundo a ISO 27005 (2011), é o processo de comparação dos resultados da análise de risco com critérios de risco previamente definidos, com o objetivo de determinar se o risco é ou não aceitável.

A Figura 6 apresenta o processo de gestão de riscos de segurança da informação definido pela ISO 27005 (2011).

Figura 6 – Processo de gestão de riscos de segurança da informação.



Fonte: ISO 27005 (2011).

O primeiro passo no processo de gestão de risco é a definição de um contexto, o que indica que o ambiente físico, tecnológico e humano influencia diretamente na gestão de risco. Após a definição do contexto, inicia-se um processo de avaliação de riscos. Este processo compreende a identificação dos riscos, a análise dos riscos e a avaliação dos riscos. O processo de avaliação dos riscos é realizado até que sejam gerados resultados satisfatórios, ou seja, sejam gerados resultados capazes de apontar ações necessárias para a redução dos riscos. Os resultados do processo de avaliação dos riscos são aplicados à etapa de tratamento dos riscos e, após a realização dos devidos tratamentos, os riscos resultantes são considerados aceitos pelo contexto previamente estabelecido.

NIST (2012) também descreve um processo de gestão de risco, o qual é compatível com o processo definido por ISO 27005 (2011). O processo de gestão de risco definido por NIST (2012) define as seguintes etapas:

- Contexto do risco: corresponde à etapa de definição de contexto da ISO 27005;
- Avaliação de risco: corresponde ao processo de avaliação de risco da ISO 27005;
- Resposta ao risco: corresponde ao processo de tratamento de risco da ISO 27005.

As seções a seguir detalham cada uma das etapas do processo de gestão de risco da ISO 27005.

2.3.1 Definição do Contexto

A definição do contexto consiste no levantamento prévio de todas as informações organizacionais relevantes para a gestão do risco de segurança da informação. Um ponto inicialmente importante na definição do contexto é o estabelecimento do escopo da gestão de risco, ou seja, quais serão os limites da organização que farão parte do processo de avaliação de risco. O escopo pode ser estabelecido em termos de produtos ou serviços específicos, ou em termos de departamentos ou setores da organização.

Os produtos, serviços, setores ou departamentos de uma organização relacionam-se com diversos ativos de informação. Ativos de informação são informações que possuem valor para a organização (ISO 27002, 2013). Estas informações caracterizam-se por gerar danos ou prejuízos para a organização caso tenham sua confidencialidade, integridade ou disponibilidade violadas.

Outro ponto importante na definição do contexto é o estabelecimento do propósito da gestão de risco, ou seja, quais são os objetivos da gestão de risco para a organização. Alguns objetivos podem ser:

- Fornecer segurança da informação à algum produto ou serviço específico;
- Atendimento a questões legais;
- Definir base para o desenvolvimento de um plano de continuidade de negócios;
- Definir base para o desenvolvimento de uma política de segurança da informação.

O estabelecimento de um contexto para gestão de risco também compreende a definição de critérios de gestão de risco. Devem-se definir critérios de impacto, avaliação e aceitação dos riscos.

Os critérios de impacto estabelecem os parâmetros que serão considerados para se classificar o montante de danos ou custos causados à organização decorrentes de um evento relacionado à segurança da informação. Um parâmetro importante para a definição do impacto é o nível de classificação ou criticidade do ativo de informação afetado por determinado evento. A violação das propriedades de confidencialidade, integridade e disponibilidade em um ativo de informação é diretamente proporcional ao impacto causado à organização.

Outros parâmetros que podem ser considerados na definição de critérios de impacto são: a parada de operações, dano à reputação, violação de questões legais e perda financeira direta.

Os critérios de avaliação de risco definem os parâmetros que serão considerados durante a avaliação dos riscos. Estes critérios podem considerar: o valor estratégico de determinados processos, a criticidade de ativos de informação e/ou expectativas de clientes e partes interessadas.

Os critérios de aceitação de riscos definem os parâmetros que serão considerados para se aceitar ou não um determinado risco. Estes parâmetros levam em conta estratégias, objetivos e políticas organizacionais. A definição de uma escala para aceitação de risco pode considerar: a relação entre o impacto de um risco e seu custo de tratamento, necessidades de clientes e partes interessadas e/ou conformidade com questões legais.

2.3.2 Identificação de Riscos

A identificação dos riscos consiste no levantamento dos elementos que possibilitam a posterior análise e avaliação dos riscos. Considerando que o risco é a combinação entre o impacto (consequências) gerado por um evento e a probabilidade da ocorrência deste evento, faz-se nesta etapa a identificação dos elementos que geram as variáveis de impacto e probabilidade.

O impacto é decorrente dos efeitos negativos causados pela perda de disponibilidade, integridade e confidencialidade sobre os ativos de informação, logo, o primeiro conjunto de componentes a ser identificado são os ativos de informação.

Ativos de informação podem compreender o hardware e software do escopo alvo da análise de risco, além de informações digitais

(arquivos), informações físicas (em papel) e ambientes físicos (salas, armários, gavetas, etc). Todos os ativos de informação envolvidos na análise de risco devem ser claramente identificados nesta fase, para posterior análise.

A probabilidade é decorrente de cenários de incidente, ou seja, a variável de probabilidade da análise de risco define a chance de ocorrência de determinado cenário de incidente. Um cenário de incidente é definido por uma determinada ameaça que explora uma determinada vulnerabilidade do escopo em questão (ISO 27005, 2011). Sendo assim, faz-se necessária a identificação das ameaças e vulnerabilidades existentes no escopo da análise de risco.

Ameaças são conceituadas como uma causa potencial de um evento indesejado (ISO 27002, 2013). As ameaças também podem ser compreendidas como sendo os agentes ou condições geradores de incidentes. Vulnerabilidades são conceituadas como fragilidades de um ativo ou grupo de ativos de informação (ISO 27002, 2013). As vulnerabilidades são exploradas por ameaças com o objetivo de se prejudicar os princípios de confidencialidade, integridade e disponibilidade dos ativos de informação, gerando assim incidentes de segurança da informação e impactos negativos aos proprietários dos ativos de informação.

A identificação de ameaças pode ser realizada através de catálogos de ameaças, consulta aos proprietários de ativos de informação ou consulta a especialistas ou grupos especializados em segurança da informação.

A identificação de vulnerabilidades pode ser realizada através de ferramentas específicas de levantamento de vulnerabilidades ou inspeção em ambientes físicos, hardwares e softwares. A identificação dos controles existentes no escopo da análise de risco também é uma importante entrada para a identificação de vulnerabilidades, visto que a ausência de controles de segurança da informação pode gerar vulnerabilidades sobre os ativos de informação.

Uma vez identificados os ativos de informação, as ameaças e as vulnerabilidades de determinado escopo, faz-se a identificação das consequências ou impactos possíveis advindos da correlação entre ameaças, vulnerabilidades e ativos de informação. O resultado da identificação de consequências é uma relação contendo cenários de incidentes (ameaças que exploram determinadas vulnerabilidades) e as consequências caso estes cenários se realizem (impactos sobre ativos de informação).

A correta identificação de ativos de informação, ameaças, vulnerabilidades e consequências é essencial para a próxima etapa do processo de avaliação dos riscos, a análise de riscos.

2.3.3 Análise de Riscos

A análise dos riscos consiste na determinação de um nível ou grau de risco para as combinações de ativos de informação, ameaças e vulnerabilidades previamente identificadas. Para tanto, faz-se uma avaliação qualitativa ou quantitativa de cada um destes elementos (ativos de informação, ameaças e vulnerabilidades).

A análise qualitativa faz uso de escalas qualificadoras para atribuição de valores de qualidade (ex. baixo, médio, alto, crítico) relacionados aos impactos (decorrentes dos ativos de informação) e probabilidades (decorrentes de ameaças e vulnerabilidades) de cenários de incidentes, já a análise quantitativa utiliza escalas de valores numéricos claramente definidos.

Uma análise qualitativa pode se basear em diversos parâmetros a fim de reduzir a subjetividade inerente a seu próprio modo de análise, porém nesta forma de análise certo nível de subjetividade sempre estará presente.

Análises quantitativas utilizam dados históricos e valores precisos objetivamente definidos, como quantidade (real) de incidentes gerados por determinada ameaça em determinado tempo ou custo (real) decorrente de determinado impacto. A grande dificuldade no desenvolvimento de análises quantitativas é a existência de valores históricos ou precisos para a realização de tal análise, fato que torna muitos escopos passíveis apenas de análises qualitativas.

A avaliação de consequências (ou impactos) ocorre através da valoração qualitativa ou quantitativa dos ativos de informação, para tal, a criticidade dos ativos de informação deve ser avaliada em termos de importância para os objetivos de negócio da organização. Alguns parâmetros para a avaliação da criticidade de ativos de informação são o valor de reposição dos ativos e as consequências ao negócio decorrentes da perda de confidencialidade, integridade e/ou disponibilidade do ativo.

A avaliação de probabilidades ocorre decompondo-se o cenário de incidente nas ameaças e vulnerabilidades que o formam e realizando-se uma avaliação (qualitativa ou quantitativa) individual de ameaças e vulnerabilidades. Ao final deste processo forma-se novamente o cenário de incidente e obtém-se a probabilidade do respectivo cenário.

As ameaças são avaliadas em termos da frequência com que ocorrem ou da exposição dos ativos de informação em relação a cada ameaça. Alguns parâmetros indicados para a avaliação das ameaças são:

- Motivação e competência dos invasores;
- Histórico de ocorrência;
- Poder atrativo dos ativos de informação envolvidos com a ameaça;
- Fatores geográficos; e
- Fatores climáticos.

As vulnerabilidades são avaliadas em termos de facilidade com que podem ser exploradas e gravidade da falha de segurança que proporcionam à ameaça.

Uma vez avaliados os ativos de informação, ameaças e vulnerabilidades, e determinados seus respectivos impactos e probabilidades, faz-se a determinação do nível ou grau de risco da cada cenário de incidente.

O nível de risco é determinado pela combinação do impacto com a probabilidade em um determinado cenário de incidente. Combinando-se impacto e probabilidade, classifica-se o risco a partir de uma matriz de risco, conforme exemplo de matriz de risco apresentado na Figura 7.

Figura 7 – Exemplo de matriz de risco.

	Probabilidade do cenário de incidente	Muito baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito Alta (Frequente)
Impacto ao Negócio	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

Fonte: ISO 27005 (2011).

Na Figura 7 o impacto e a probabilidade foram avaliados de modo qualitativo e a combinação destas duas variáveis classifica o risco em uma escala de zero a oito. Esta matriz de risco define três faixas para classificação do nível de risco, que poderiam ser interpretadas como:

- Risco baixo, quantificado de zero a dois;
- Risco moderado, quantificado de três a cinco; e
- Risco alto, quantificado de seis a oito.

A ISO 27005 (2011) apresenta e discute várias abordagens para a análise de riscos e vários exemplos de matriz de risco. Porém é importante destacar que seu objetivo não é apresentar um roteiro ou metodologia para a realização da análise de risco, mas sim discutir diretrizes gerais para a realização desta.

2.3.4 Avaliação de Riscos

Após a etapa de definição dos níveis de risco para os cenários de incidentes, ocorre a avaliação dos riscos. Nesta etapa os cenários de incidentes e seus respectivos níveis de risco devem ser avaliados com base nos critérios de avaliação de riscos definidos na fase de definição do contexto.

Os riscos resultantes da fase de análise de riscos podem ser avaliados sob o aspecto das propriedades de segurança da informação, por exemplo, para algumas organizações a disponibilidade será mais importante que a confidencialidade, e desta forma os riscos envolvendo vulnerabilidades de disponibilidade devem ser priorizados.

Outra forma de avaliação dos riscos é sob o aspecto da importância de processos de negócio. Para algumas organizações certos processos de negócio ou serviços têm prioridade sobre outros. Desta forma os riscos relacionados com os processos de negócio ou serviços prioritários devem receber destaque em relação aos riscos relacionados com processos de negócio menos prioritários.

Na fase de avaliação dos riscos estes também devem ser comparados com os critérios para aceitação dos riscos e devem ser classificados em riscos aceitáveis ou não.

A saída da fase de avaliação de riscos é uma relação dos riscos previamente analisados, porém agora ordenada com base nos critérios de avaliação de risco.

2.3.5 Tratamento do Risco

A fase de tratamento do risco classifica ações para os riscos previamente identificados, analisados e avaliados. A Figura 8 apresenta as opções de tratamento de riscos definidas pela ISO 27005 (2011).

Figura 8 – Opções de tratamento do risco.

Fonte: ISO 27005 (2011).

Com base na Figura 8 os riscos avaliados podem ser:

- Modificados: consiste na implementação ou alteração de controles de segurança da informação de modo que o risco em questão seja mitigado. A ISO 27002 (2013) apresenta e discute uma série de objetivo de controle e controles de segurança da informação para a redução de riscos;
- Retidos (ou aceitos): caso o nível de risco atenda aos critérios de aceitação de risco, este poderá ser aceito, ou seja, define-se que não serão realizadas ações relativas ao risco em questão;
- Evitados: consiste na eliminação completa da causa do risco. Muitas vezes esta opção de tratamento está ligada a questões

de localização geográfica. Um exemplo de ação para se evitar o risco é a mudança de um local de processamento de informações sujeito a inundações para outro local não sujeito a tais condições naturais.

- Compartilhados: consiste em dividir o risco com entidades externas. Um exemplo de compartilhamento de risco é a contratação de seguros. Outro exemplo é a contratação de fornecedores que se responsabilizam por controles ou ações que reduzem a probabilidade ou impacto de determinado risco. O compartilhamento do risco com fornecedores pode criar novos riscos, pois o ambiente do fornecedor pode oferecer novas ameaças ou vulnerabilidades.

Entre as quatro opções de tratamento de risco a modificação é a mais utilizada no caso de riscos inaceitáveis. A retenção somente deveria ser utilizada em casos de riscos aceitáveis, conforme critérios para aceitação de riscos. A realização de ações para se evitar o risco e o compartilhamento de riscos são tratamentos mais limitados, pois o primeiro somente pode ser aplicado a casos específicos e o segundo pode gerar novos riscos.

2.4 TRABALHOS RELACIONADOS

Esta seção apresenta diversos trabalhos relacionados com esta tese. A apresentação dos trabalhos relacionados está dividida em três grupos. O primeiro grupo apresenta estudos relacionados com elementos que compõem uma análise de risco, como estudos relacionados com ameaças, vulnerabilidades e requisitos de segurança da informação. Estes estudos servem de base para a identificação de riscos, conforme descrito na seção 2.3.2.

O segundo grupo apresenta avaliações de segurança da informação aplicadas à computação em nuvem e que tenham como base a ISO 27001. Estas avaliações de segurança com base na ISO 27001 são correlatas a esta tese no sentido de que também fornecem elementos para a identificação de riscos específicos de ambientes de nuvem.

O terceiro grupo apresenta trabalhos relacionados especificamente com a análise de risco em ambientes de computação em nuvem, sendo estes baseados ou não na ISO 27001.

2.4.1 Identificação de Riscos em Nuvem

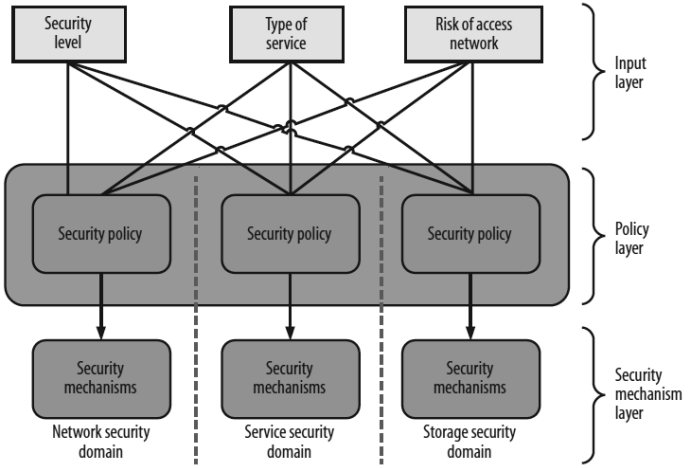
Rot (2013) discute novas ameaças de segurança da informação aplicadas especificamente em ambientes de computação em nuvem. O levantamento realizado afirma que a cada momento surgem novas ameaças relacionadas à computação em nuvem e que a constante avaliação destas ameaças é necessária para garantir a segurança de informações e serviços na nuvem.

O trabalho de Rot (2013) comenta os desafios para a segurança da computação em nuvem, entre eles: a complexidade da tecnologia, o fornecimento de ferramentas de segurança pelos provedores e as ameaças inerentes a internet.O artigo também apresenta uma relação de classificação de ameaças para sistemas de tecnologia da informação, como: ameaças relacionadas com dados, sistemas computacionais e ameaças de perdas financeiras.

Zhang (2012) apresenta um estudo sobre os principais fatores que afetam a segurança da informação em ambientes de nuvem. Além disto, analisa a importância de se realizar análises e avaliações de risco de segurança da informação em ambientes de nuvem. Enquanto Luna (2012) aborda o uso de políticas quantitativas para acordos de nível de serviços de segurança da informação em nuvem. O artigo propõe um método para avaliação de requisitos de segurança do cliente da nuvem em um ou mais CSPs. O método proposto fornece uma estrutura de dados para representação dos SecLAs (Security Level Agreement).

Chen (2012) considera que a computação em nuvem oferece grandes obstáculos à segurança da informação e que a execução de avaliações de segurança por entidades externas ao CSP é um importante controle de segurança para a redução destes obstáculos. Destaca também que o estudo da segurança em nuvem ainda é inicial, pois não existe um modelo ou conjunto de técnicas universalmente aceito. A arquitetura de segurança para nuvem proposta por Chen (2012) fornece segurança sob demanda aplicando diferentes algoritmos e protocolos durante três estágios do ciclo de vida dos serviços de nuvem: transmissão, processamento e armazenamento.

Figura 9 – Arquitetura de segurança sob-demanda.



Fonte: CHEN (2012).

A Figura 9 apresenta a arquitetura de segurança sob-demanda proposta por Chen (2012). A camanda de *input* recebe os dados de entrada do modelo de segurança, a camada de *policy* define os parâmetros de segurança que serão aplicados ao ambiente alvo, enquanto a camada de mecanismos de segurança aplica proteção aos serviços específicos do ambiente alvo, conforme as instruções recebidas pelas duas camadas anteriores.

Bleikertz (2013) cita que apesar de existirem várias partes envolvidas no fornecimento de serviços de nuvem, o cliente da nuvem ainda possui muita dificuldade em avaliar as ameaças, vulnerabilidades e riscos do ambiente de nuvem que consome. São então necessários modelos que permitam a avaliação sistemática do CSP por parte do CC. Bleikertz (2013) propõe um modelo de alto nível para CCs avaliarem a segurança de CSPs. O modelo é baseado na descrição de cenários *"what-if"* e na sistemática avaliação destes cenários no ambiente de nuvem.

2.4.2 Avaliações da ISO 27001 para Nuvem

Ristov (2012) propõe um modelo para avaliação de segurança da informação em ambientes de computação em nuvem com base na ISO

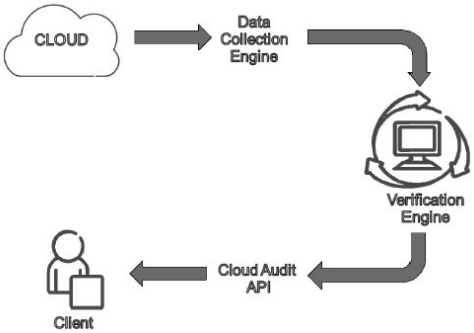
27001. Este modelo consiste em uma extensão da ISO 27001 de modo que esta atenda aos requisitos específicos de ambientes de computação em nuvem, como por exemplo, a virtualização.

Ristov (2013) apresenta uma avaliação de segurança dos principais ambientes de nuvem de código aberto. O estudo analisou os ambientes OpenStack, Eucalyptus, OpenNebula e CloudStack considerando aspectos de segurança definidos pela ISO 27001, como: estabilidade, implementação, operação, monitoramento e revisão. O estudo mostra que todos os ambientes avaliados apresentam inconformidade com grande parte dos requisitos da ISO 27001.

Uma avaliação de segurança em nuvem com base na ISO 27001 também é apresentada por Mirkovié (2013). O artigo apresenta alguns controles de segurança da informação da ISO 27001 aplicados à computação em nuvem, além de métricas de segurança para tais controles.

Bhensook (2012) e Ullah (2013) descrevem o esforço da CSA – Cloud Security Alliance para automação da avaliação de segurança da informação em CSPs, o CloudAudit. Bhensook (2012) comenta que a avaliação de segurança em CSPs é importante para o CCs identificarem se um ambiente de nuvem atende aos requisitos de segurança de seu negócio. Ullah (2013) comenta que a falta de conformidade com requisitos e norma de segurança é o obstáculo que mais impede a adoção de soluções de nuvem pelas empresas. O CloudAudit visa automatizar vários aspectos da avaliação de segurança da informação em ambientes de computação em nuvem. Tanto Bhensook (2012) quanto Ullah (2013) utilizam como base a ISO 27001 para o desenvolvimento de seus modelos.

Figura 10 – Visão de alto nível da arquitetura Cloud Audit.



Fonte: ULLAH (2013).

A Figura 10 apresenta uma visão de alto nível da arquitetura de Cloud Audit proposta por Ullah (2013). O primeiro passo para verificação de conformidade é a colea de dados do provedor de nuvem. Em seguida ocorre a verificação dos dados coletados, através da máquina de verificação. O último passo é a entrega dos dados de auditoria ao cliente, para sua avaliação de conformidade.

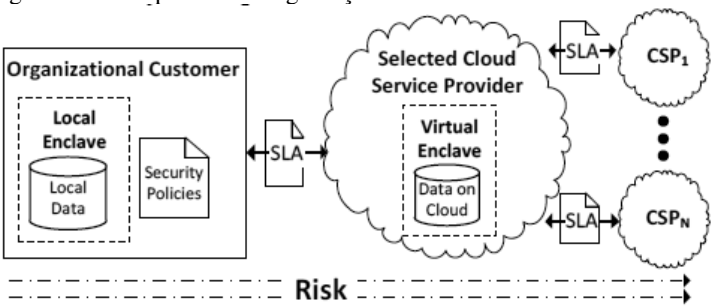
Alebrahim (2014) comenta que a segurança da informação é uma questão essencial para tomada de decisão na aquisição de serviços de computação em nuvem e que a ISO 27001 fornece um padrão geral para o tratamento desta questão. Comenta também que análise de risco é uma parte essencial da ISO 27001, sendo assim, propõe um método estruturado para a identificação de ativos de informação, ameaças e vulnerabilidades.

2.4.3 Análise de Risco em Nuvem

Morin (2012) destaca que um grande desafio para os ambientes de computação em nuvem é a conformidade com normas de governança e gerenciamento de risco. Em seu artigo Morin (2012) cita os desafios de se propor um modelo para gerenciamento de risco para computação em nuvem e comenta especificamente sobre a proposição de soluções para o estabelecimento de SLAs de risco para ambientes de computação em nuvem.

Hale (2012) descreve um framework chamado SecAgreement. O SecAgreement realiza o cálculo do risco de um CSP a partir de métricas de segurança pré-definidas pelo CC. O framework também determina GAPs de segurança entre a métrica e a estrutura do CSP.

Figura 11 – Perspectiva de segurança em nuvem.



Fonte: HALE (2012).

A Figura 11 apresenta a arquitetura de segurança em nuvem SecAgreement proposta por Hale (2012). Nesta arquitetura existe a definição de um SLA para contratação do serviço de nuvem. O CSP então fornece o monitoramento deste SLA para o cliente de nuvem, que avalia a qualidade conformidade do serviço prestado.

Zech (2012) apresenta um modelo para análise de risco para computação em nuvem com base em testes de segurança. O modelo apresentado tem como diferencial a especificação de testes de requisitos negativos e casos de uso incorretos. O modelo de Zech (2012) também considera as interfaces externas da nuvem como um importante ponto de vulnerabilidade e analisa o risco de exploração desta vulnerabilidade específica da nuvem.

Wang (2012) explora a análise de risco em computação em nuvem através do desenvolvimento de grafos de ataque e defesa. A análise de risco de Wang (2012) verifica o custo para um ataque em relação ao custo para sua respectiva defesa e a partir disto determina o grau de risco do CSP. Para os cenários de risco Wang (2012) faz uso da base de vulnerabilidades *CVE – Common Vulnerabilities and Exposures*.

Khosravani (2013) apresenta um estudo de caso de análise de risco em computação em nuvem. O estudo apresenta grande foco na importância dos requisitos de segurança dos dados que serão migrados para a nuvem (os ativos de informação), ou seja, foca no risco considerando as necessidades do CC. São apresentados os principais riscos e controles específicos para o estudo de caso em questão.

Lenkala (2013) destaca que muitos estudos têm sido desenvolvidos na área de segurança em nuvem com foco em vulnerabilidades de camadas operacionais e que a segurança do caminho que leva o CC ao CSP tem sido pouco estudada. O artigo apresenta um modelo e métricas para realização de análise e avaliação de riscos especificamente relacionados com o caminho entre o CC e o CSP. O objetivo é que o CC possa avaliar qual CSP apresenta o caminho mais seguro para suas informações e serviços. O modelo apresentado usa como base a *NVD – National Vulnerability Database* para identificação de vulnerabilidades.

Liu (2013) propõe um modelo para análise de risco de segurança da informação em máquinas virtuais de ambientes de computação em nuvem. O modelo de Liu (2013) baseia-se nos conceitos apresentados pelas normas ISO 270001, 27002 e 27005. O artigo também apresenta o desenvolvimento de um protótipo para a plataforma OpenStack e resultados experimentais.

Cayirci (2014) apresenta um modelo para avaliação de risco em nuvem no qual o cliente possa realizar a avaliação e analisar o risco da adoção de determinado provedor de nuvem. O autor comenta que esta é uma abordagem essencial para que o cliente de nuvem possa realizar a tomada de decisão mais adequada em relação ao seu perfil de risco.

Madria (2015) comenta que questões relacionadas com segurança da informação estão entre as primeiras razões para que as organizações evitem a adoção de serviços de computação em nuvem. O artigo apresenta um modelo para avaliação de risco do CSP, considerando o nível de segurança oferecido para uma determinada aplicação alocada em seu ambiente.

Gupta et al. (2015) destacam que é cada vez maior a quantidade de provedores de serviços de nuvem disponíveis no mercado, fornecendo os mais diversos tipos de serviços. Este fato apenas torna mais complicada a decisão sobre a adoção de determinado provedor de nuvem por parte do cliente. Sendo assim, é cada vez maior a quantidade de pesquisas que visam fornecer ao CC informações para o suporte a sua decisão de escolha quanto a seu provedor de nuvem. O autor trabalha sob a abordagem de sistemas de suporte à decisão para uma análise dos riscos da seleção de determinado provedor de nuvem. Ao final, com objetivo de prova de conceito, o artigo apresenta um protótipo do modelo proposto.

2.5 DISCUSSÃO DOS TRABALHOS RELACIONADOS

Os trabalhos correlatos acima apresentados discutem modelos e definições de requisitos para análise de risco em computação em nuvem, porém eles não atuam na definição dos agentes envolvidos e suas interações durante a execução da análise de risco. Eles também não apresentam formas de atualização constante, colaboração, representação ou evolução dos requisitos de segurança, que muitas vezes estão descritos de modo estático.

As soluções de análise de risco para computação em nuvem identificadas nos trabalhos relacionados apresentam diferentes níveis de limitação nos aspectos de abrangência, aderência e independência da análise de risco. O aspecto de abrangência relaciona-se com a definição do escopo dos requisitos de segurança aplicados à análise de risco. O aspecto de aderência consiste em considerar a natureza do negócio do cliente no cálculo da análise de risco. O aspecto de independência consiste em realizar a análise de risco de tal modo que sua

especificação, execução e resultados não sejam influenciados por interesses de agentes específicos, como por exemplo o CSP.

O Quadro 1 apresenta a relação de cada um dos trabalhos correlatos com os aspectos de abrangência, aderência e independência.

Quadro 1 – Relação dos trabalhos correlatos com os aspectos estudados.

Referência	Abrangência	Aderência	Independência
Rot (2013)	X		
Zhang (2012)	X		
Luna (2012)		X	
Chen (2012)			X
Bleikertz (2013)			X
Ristov (2012)	X		
Ristov (2013)	X		
Mirkovié (2013)	X		
Bhensook (2012)	X		X
Ullah (2013)	X		X
Alebrahim (2014)	X	X	
Morin (2012)			X
Hale (2012)		X	
Zech (2012)	X		
Wang (2012)	X		
Khosravani (2013)		X	
Lenkala (2013)			X
Liu (2013)			X
Cayirci (2014)		X	
Madria (2015)			X
Gupta (2015)	X		

Fonte: própria.

As limitações de abrangência, aderência e independência dos modelos atuais de análise de risco em nuvem geram deficiências, como:

- **Deficiência na Abrangência dos Requisitos**: ocorre quando a seleção dos requisitos de segurança é limitada, como por exemplo, quando é realizada pelo próprio CSP ou por um

agente sem conhecimento suficiente. O CSP pode especificar requisitos de segurança viciados em seu próprio ambiente, fraudando assim os resultados da análise de risco. Já um agente despreparado pode especificar requisitos insuficientes ou desconsiderar algum requisito importante, gerando assim uma análise de risco incorreta;

- **Deficiência na Aderência ao Cliente**: ocorre quando não existe a definição de impactos gerados ao CC por um incidente de segurança ou quando o agente responsável pela definição de impactos desconhece o ambiente tecnológico e a natureza de negócio do CC. Neste caso a especificação do impacto pode desconsiderar cenários relevantes para o CC ou superestimar cenários não relevantes, gerando assim uma avaliação de risco incorreta;
- **Deficiência na Independência dos Resultados**: ocorre quando a quantificação das probabilidades e impactos é realizada por um agente que tem interesse em minimizar os resultados da análise de risco. Por exemplo, se a análise for executada unicamente pelo CSP este pode suavizar a avaliação dos requisitos e impactos, gerando assim um resultado satisfatório para o CC, porém incorreto.

As deficiências acima apresentadas geram uma falta de confiança por parte dos CCs em relação às análises de risco realizadas nos CSPs, pois nos modelos atuais os próprios CSPs realizam suas próprias análises de risco, sem a participação ativa dos CCs (por exemplo, de definição de impactos) ou qualquer outro agente externo.

Os aspectos de definição e interação dos agentes envolvidos na análise de risco, inclusive considerando a colaboração de entidades externas na definição de requisitos de segurança, bem como a atualização e evolução dos requisitos de segurança e a execução contínua da análise de risco nos CSPs pelos CCs são o foco de atuação deste trabalho de tese.

3 MODELO PROPOSTO – RACLOUD

A primeira seção deste capítulo descreve uma contextualização do modelo proposto. O modelo proposto, nomeado *RACloud – Risk Analysis for Cloud*, é composto por uma modelagem de risco, uma linguagem de definição de risco e uma arquitetura organizada em componentes. A segunda seção deste capítulo apresenta a modelagem de risco desenvolvida para o modelo proposto. A seção 3.3 descreve a linguagem de definição de risco desenvolvida a partir da modelagem de risco. A quarta seção apresenta os componentes da arquitetura do modelo proposto, que fará uso da modelagem de risco e da linguagem de definição de risco.

3.1 CONTEXTUALIZAÇÃO DO MODELO PROPOSTO

A abordagem proposta por este trabalho segue a linha do desenvolvimento de padrões para interoperabilidade de serviços de nuvem, especificamente para área de análise de risco em segurança da informação. Cloud Security Alliance (2011) destaca o surgimento recente de muitos esforços no sentido do desenvolvimento de interfaces ao mesmo tempo abertas e proprietárias que busquem permitir recursos como o gerenciamento, segurança e interoperabilidade para a nuvem. Alguns desses esforços incluem o grupo de trabalho Open Cloud Computing Interface Working Group, a API da Amazon EC2, a API vCloud da Vmware, submetida ao DMTF (Distributed Management Task Force), a API Open Cloud da Sun, a API da Rackspace e a API da GoGrid. Modelos de interfaces abertas e padronizadas terão um papel fundamental na portabilidade e interoperabilidade da nuvem, assim como formatos genéricos padronizados como o Open Virtualization Format (OVF) da DMTF (CLOUD SECURITY ALLIANCE, 2011).

A conectividade onipresente e a ineficácia dos controles estáticos de segurança, que não conseguem tratar da natureza dinâmica dos serviços de nuvem, geram a necessidade de novos modelos de segurança para computação em nuvem (CLOUD SECURITY ALLIANCE, 2011).

Considerando também que ameaças e códigos maliciosos internos são as fontes de incidentes de segurança mais comuns e de maior risco nos ambientes de computação em nuvem (CLOUD SECURITY ALLIANCE, 2011), faz-se necessário o desenvolvimento de novos modelos de segurança que incluam agentes externos no processo de análise de risco de segurança da informação em nuvem.

A abordagem proposta neste trabalho para permitir a análise de risco de segurança da informação do CSP pelo CC é a construção de um modelo computacional de análise de risco para ambientes em nuvem, que possibilite ao CC a execução de uma análise de risco de modo abrangente, aderente e independente. O modelo proposto será referenciado como *"RACloud – Risk Analysis for Clouds"*.

Para atender à necessidade de dinamismo destacada pela CSA o modelo proposto deve permitir a representação, atualização e execução de modelos dinâmicos de risco. Esta característica gera a necessidade do modelo proposto disponibilizar uma linguagem para representação do risco e suas variáveis.

Srinivasan (2012) comenta que CCs que falham na especificação de seus requisitos de segurança para computação em nuvem podem sofrer incidentes graves sem poder posteriormente responsabilizar o CSP. Este fato relaciona-se com o aspecto de abrangência a ser trabalhado no modelo proposto.

Para atender ao aspecto de abrangência o modelo proposto deve possibilitar a participação de entidades externas especializadas em segurança da informação. Deve ainda possibilitar a representação computacional das variáveis integrantes de uma análise de risco e permitir a atualização constante das definições de risco.

Segundo Zhang (2010) o impacto causado por diferentes cenários de incidentes pode variar entre CCs, conforme a natureza e objetivos de seu negócio. Este fato relaciona-se com o aspecto de aderência a ser trabalhado no modelo proposto. Sendo assim, o modelo proposto deve considerar a participação dos CCs na definição e quantificação de impactos decorrentes de cenários de incidentes, com o intuito de aprimorar o aspecto de aderência ao negócio do cliente durante a especificação e execução da análise de risco.

Segundo Ristov (2012) os CCs sabem que existem benefícios e riscos na adoção de uma solução de computação em nuvem. Para eles é importante que os benefícios sejam superiores aos riscos, e uma análise de risco independente pode auxiliar nesta avaliação. Para atuar no aspecto de independência o modelo proposto deve identificar os agentes envolvidos na análise de risco e atribuir as responsabilidades mais adequadas a cada agente. Considerando que o CSP é o agente que está sendo avaliado pela análise de risco, este deve ter suas responsabilidades restringidas ao máximo dentro das atribuições do modelo proposto.

A Cloud Security Alliance (2011) ainda destaca que uma análise de risco deve considerar:

- Os ativos de informação gerenciados pela nuvem;

- Quem gerencia e como os ativos são gerenciados;
- Os controles de segurança selecionados pelo CSP e como estes controles estão integrados entre si;
- Questões relacionadas com normas e conformidade de segurança da informação.

Com base nas recomendações acima citadas o modelo proposto também deve dar grande atenção às características dos ativos de informação envolvidos na análise de risco, bem como considerar a recomendação de normas de segurança da informação, como as normas ISO/IEC 27001 (2013), ISO/IEC 27002 (2013) e ISO/IEC 27005 (2011), que tratam respectivamente da gestão de segurança da informação, seleção de controles de segurança da informação e análise de risco em segurança da informação. Sendo assim, o modelo proposto irá tomar como base em sua análise de risco a família de normas ISO 27000, mais especificamente a ISO 27005 (ISO 27005, 2011).

3.2 MODELAGEM DO RISCO

Esta seção apresenta a definição do modelo RACloud para níveis de risco, categorias de recursos em nuvem e categorias de ativos de informação. Também é apresentada a especificação do modelo RACloud para risco, eventos e elementos básicos de risco, como ameaças, vulnerabilidades e ativos de informação.

3.2.1 Níveis de Risco

Inicialmente o modelo de risco para computação em nuvem RACloud define quatro Níveis de Risco (*RL – Risk Level*) nos quais os riscos podem estar presentes, sendo estes os seguintes:

- **RL 0 (Hardware)**: representa especificamente os hardwares de um ambiente de computação em nuvem. Neste nível podem ser encontrados riscos relacionados com recursos como CPU, memória ou discos de armazenamento;
- **RL 1 (Infraestrutura)**: representa o nível de IaaS conforme modelos de serviço para computação em nuvem (CSA, 2011). Neste nível podem ser encontrados riscos relacionados com recursos como o sistema operacional, sistemas de virtualização, sistemas de comunicação ou sistemas de armazenamento (ex. storage);

- **RL 2 (Plataforma)**: representa o nível de PaaS conforme modelos de serviço para computação em nuvem (CSA, 2011). Neste nível podem ser encontrados riscos relacionados com recursos como sistemas de banco de dados, frameworks de desenvolvimento (ex. java, C++) ou servidores de aplicação (ex. servidores web ou containers web services);
- **RL 3 (Software)**: representa o nível de SaaS conforme modelos de serviço para computação em nuvem (CSA, 2011). Este nível apresenta riscos potenciais específicos de sistemas aplicativos (ex. sistema multimídia) ou sistemas de informação (ex. sistemas de vendas ou de gerenciamento de projetos).

A organização dos riscos em níveis é importante para posterior correlação entre ativos de informação, ameaças e vulnerabilidades, ou seja, para identificação de quais ameaças exploram quais vulnerabilidades e quais ativos de informação são impactados por determinado incidente de segurança.

Cada RL definido pelo modelo RACloud é composto por uma série de recursos de tecnologia da informação. Estes recursos podem armazenar ativos de informação, possuir vulnerabilidades ou mesmo serem explorados por ameaças para a geração de incidentes de segurança da informação. Desta forma, os recursos de tecnologia da informação existentes em cada nível de risco são elementos importantes para uma análise de risco de computação em nuvem.

No modelo RACloud os diferentes recursos existentes em um ambiente de computação em nuvem são agrupados em RCs (*Resource Category*). Conforme descrito no Quadro 2, são definidos 10 RCs no modelo RACloud. Estes RCs serão utilizados posteriormente na análise de risco para se fazer a correlação entre ativos de informação, ameaças e vulnerabilidades.

Quadro 2 – Categorias de recurso do modelo RACloud.

RC	RL	Exemplos de Recursos
Hardware	0	CPU, memória, disco
SO System	1	Windows, linux
VM System	1	Vmware, HiperV
Communication System	1	IP, TCP, UDP, HTTP
Cloud System	1	Amazon S3, Rackspace Cloud Files
Database	2	Oracle, MySQL, Amazon SimpleDB
Framework	2	Java, C#, etc
Application Server	2	Amazon AWS
Application System	3	Office 365
Information System	3	Sale force

Conforme descrito no Quadro 2, Hardware é uma categoria de recursos pertencente ao RL 0-Hardware que abrange elementos físicos como CPU, memória ou discos de armazenamento. O nível de risco 1-Infraestrutura fornece recursos como os sistemas operacionais, sistemas de virtualização e sistemas de comunicação, além de sistemas específicos para o funcionamento e gerenciamento de ambientes de computação em nuvem.

Para o nível de risco 2-Plataforma o modelo RACloud define como recursos os sistemas de gerenciamento de banco de dados (RC Database); as bibliotecas e ambientes de desenvolvimento de sistemas (RC Framework) e os ambientes de execução de sistemas (RC Application Server). Sistemas utilizados, desenvolvidos e/ou alocados pelo CC no ambiente do CSP farão uso e estarão sujeitos às vulnerabilidades e ameaças decorrentes destes recursos.

Os sistemas aplicativos e os sistemas de informação fornecidos pelo CSP (de responsabilidade do CSP) ao CC são recursos do nível de risco 3-Software e são representados pelas categorias de recursos *Application System* e *Information System*, respectivamente.

Os Níveis de Riscos (RLs) relacionam-se com diferentes tipos de ativos de informação, devido ao fato de fornecerem diferentes Categorias de Recurso (RCs). O modelo RACloud organiza os diferentes tipos de ativos de informação alocados por um CC em um ambiente de computação em nuvem em quatro Categorias de Ativos (*AC – Asset Category*): (i) File, (ii) Database, (iii) CC-Software e (iv) CSP-Software.

Conforme apresenta o Quadro 3, a categoria de ativos de informação File pertence ao RL 1-Infraestrutura. Ativos de informação pertencentes a esta categoria consistem em todo e qualquer arquivo pertencente ao CC e armazenado diretamente no sistema de arquivos do CSP. Exemplos desta categoria de ativos de informação são documentos de texto, planilhas ou arquivos gráficos de qualquer tipo armazenados no sistema de arquivos do CSP.

Quadro 3 – Categorias de ativos de informação do modelo RACloud.

AC	RL	Exemplos de Ativos
File	1	Textos, planilhas, figuras
Database	2	Informações financeiras ou de clientes
CC-Software	2	Sistema de pedidos
CSP-Software	3	E-mails

A segunda categoria de ativos de informação, Database, pertence ao RL 2-Plataforma e consiste em toda e qualquer informação pertencente ao CC e armazenada em uma base de dados hospedada no ambiente de nuvem do CSP. Nestes casos a aplicação que faz uso da base de dados pode estar no ambiente do CC, do CSP ou mesmo em outro ambiente externo a ambos. Exemplos de ativos de informação pertencentes a esta categoria são informações financeiras ou informações cadastrais de cliente pertencentes a um sistema ERP específico.

A AC CC-Software pertence ao nível de risco 2-Plataforma e consiste em sistemas desenvolvidos e pertencentes ao CC, porém executados e disponibilizados a usuários do CC através do ambiente de computação em nuvem do CSP. No caso desta categoria de ativos de

informação o sistema em si é o próprio ativo de informação do CC, e a análise de risco terá por foco identificar riscos inseridos no sistema do CC por parte do ambiente de nuvem (hardware, infraestrutura ou plataforma) do CSP.

Para o nível de risco 3-Software o modelo RACloud define a categoria de ativos de informação CSP-Software. É importante destacar que esta categoria de ativos de informação não é representada pelos softwares do CSP fornecidos ao CC, mas sim pelas informações pertencentes ao CC e que estão armazenadas em formatos específicos de softwares do CSP e são acessadas através destes softwares. Os softwares fornecidos pelo CSP não são ativos de informação do CC, pois não pertencem ao CC mais sim ao CSP. Conforme visto no Quadro 2 os softwares fornecidos pelo CSP são tratados pelo modelo RACloud como recurso (Application System e Information System) e não como ativos de informação.

3.2.2 Especificação do Risco

O modelo RACloud define o compartilhamento de responsabilidades entre três entidades durante a análise de risco: CC (Cloud Consumer), CSP (Cloud Service Provider) e o ISL (Information Security Labs). O ISL é uma entidade que representa um laboratório ou grupo de segurança da informação público, acadêmico ou privado. O CC é uma entidade que representa a entidade que hospeda seus ativos de informação na cloud. E o CSP é uma entidade que representa a entidade que será analisada, ou seja, é o provedor de recursos de computação em nuvem (SILVA, 2014).

O Quadro 4 apresenta a simbologia utilizada no modelo para representar as entidades participantes da análise de risco.

Quadro 4 – Entidades envolvidas na análise de risco.

Símbolo	Descrição
CC_x	**Cloud Consumer** "x". Representa um cliente do ambiente de computação em nuvem.
CSP_y	**Cloud Service Provider** "y". Representa um provedor de recursos de computação em nuvem.
ISL_z	**Information Security Laboratory** "z". Representa um laboratório de segurança da informação especializado na definição e análise de riscos de computação em nuvem.

As três entidades definidas no modelo RACloud dividem as responsabilidades da execução de uma análise de risco, conforme os conceitos definidos pela ISO 27005. Neste contexto ameaças exploram vulnerabilidades de modo a gerar impacto sobre ativos de informação (ISO 27005, 2011).

O modelo RACloud também prevê três propriedades de segurança da informação: confidencialidade, integridade e disponibilidade (conforme ISO 27001). O Quadro 5 apresenta a especificação simbólica das propriedades de confidencialidade, integridade e disponibilidade do modelo RACloud.

Quadro 5 – Propriedades de segurança da informação.

Símbolo	Descrição
c	Propriedade de segurança **Confidenciality**
i	Propriedade de segurança **Integrity**
a	Propriedade de segurança **Availability**

Ativos de informação, ameaças e vulnerabilidades são os elementos básicos de uma análise de risco de segurança da informação. As variáveis da modelagem de risco que representam ativos de informação, ameaças e vulnerabilidades estão representadas no Quadro 6.

As ameaças e vulnerabilidades são especificadas por uma entidade ISL, visto que esta é a entidade especializada em segurança da informação. Os ativos de informação são especificados por uma entidade CC, visto que é esta a proprietária dos ativos de informação e maior conhecedora do impacto causado por um incidente sobre determinados ativos de informação.

As categorias de recursos (RCs) vistas na seção anterior, bem como as propriedades de segurança vistas no Quadro 5 são agora importantes atributos das ameaças e vulnerabilidades (T e V respectivamente), da mesma forma que as categorias de ativos de informação se aplicam agora na definição dos ativos de informação (A, conforme Quadro 6). Estas informações serão importantes posteriormente na execução da análise de risco.

Quadro 6 – Elementos básicos da análise de risco.

Símbolo	Descrição
$T_{isl,rc,p[]}$	**Threat** especificada por determinado ISL e que atua sobre determinada categoria de recursos do CSP e determinado conjunto de propriedades de segurança
$A_{cc,ac}$	**Information Asset** especificado por determinado CC e que faz parte de determinada categoria de ativos de informação do CC
$V_{isl,rc,p[]}$	**Vulnerability** especificada por determinado ISL e que faz parte de determinada categoria de recursos do CSP e determinado conjunto de propriedades de segurança

Uma vez definidos elementos de ameaças, vulnerabilidades e ativos de informação, funções de análise são aplicadas a estes elementos (Quadro 6) com o objetivo de quantificá-los em relação às propriedades de segurança (Quadro 5).

Na função de análise dos ativos de informação quantifica-se o grau de impacto (*DI – Degree of Impact*) visto que em um cenário de concretização de um risco os ativos de informação produzem um impacto para o CC decorrente das consequências geradas pelo incidente de segurança da informação.

O impacto produzido por um incidente de segurança da informação pode ser decorrente da anulação de uma ou mais propriedades de segurança da informação (Quadro 5) necessárias para o bom funcionamento ou uso adequado do ativo de informação, sendo assim, a variável DI relaciona-se com as diferentes propriedades de segurança da informação previamente apresentadas.

O Quadro 7 apresenta a definição da função de análise de impacto para os ativos de informação, bem como a definição das variáveis de grau de impacto.

Quadro 7 – Análise e quantificação dos ativos de informação.

Símbolo	Descrição
$iaf(A_{cc,ac})$	**Impact Analysis Function** para determinados ativos de informação
$DI_{A,\{c,i,a\}}$	**Degree of Impact** de determinado do ativo de informação para cada uma das propriedades de segurança da informação $iaf(A_{cc,ac})=\{DI_{A,c}, DI_{A,i}, DI_{A,a}\}$

Para os elementos de vulnerabilidade o modelo RACloud define funções de análise para quantificação do grau de deficiência (*DD - Degree of Deficiency*). Esta variável representa o grau de deficiência potencial presente em determinado ambiente de computação em nuvem gerado pela existência de determinada vulnerabilidade.

A variável DD relaciona-se com cada uma das propriedades de segurança da informação da vulnerabilidade, desde que tal propriedade pertença ao conjunto `p[]` especificado na definição da vulnerabilidade (Quadro 6). Visto que vulnerabilidades presentes nos recursos do CSP poderão gerar diferentes níveis de deficiência no ambiente de computação em nuvem em relação às diferentes propriedades de segurança.

O Quadro 8 apresenta a definição da função de análise de deficiência para vulnerabilidades de recursos fornecidos pelo ambiente do CSP, bem como a definição das variáveis de grau de deficiência.

Quadro 8 – Análise e quantificação das vulnerabilidades.

Símbolo	Descrição
$daf(V_{isl,rc,p[]}, CSP_y)$	**Deficiency Analysis Function** para determinada vulnerabilidade aplicada a determinado CSP
$DD_{V,CSP,\{c,i,a\}}$	**Degree of Deficiency** de determinada vulnerabilidade em determinado CSP para cada uma das propriedades de segurança da informação $daf(V_{isl,rc,p[]}, CSP_y) = \{DD_{V,CSP,c}, DD_{V,CSP,i}, DD_{V,CSP,a}\}$

Para os elementos de ameaças o modelo RACloud define funções de quantificação de grau de exposição (*DE – Degree of Exposure*). Esta variável representa o nível ao qual os recursos do CSP estão expostos às diferentes ameaças de segurança da informação.

A variável DE relaciona-se com cada uma das propriedades de segurança da informação da ameaça, desde que tal propriedade pertença ao conjunto `p[]` especificado na definição da ameaça (Quadro 6). Visto que a exposição do ambiente de computação em nuvem do CSP a determinada ameaça pode afetar de modo diferente cada uma das propriedades de segurança da informação.

Quadro 9 – Análise e quantificação das ameaças.

Símbolo	Descrição
$eaf(T_{isl,rc,p[]}, CSP_y)$	**Exposure Analysis Function** para determinada ameaça aplicada a determinado CSP
$DE_{T,CSP,\{c,i,a\}}$	**Degree of Exposure** de determinada ameaça em determinado CSP para cada uma das propriedades de segurança da informação $eaf(T_{isl,rc,p[]}, CSP_y) = \{DE_{T,CSP,c}, DE_{T,CSP,i}, DE_{T,CSP,a}\}$

O Quadro 9 apresenta a definição da função de análise de exposição e das variáveis de grau de exposição das ameaças às diferentes propriedades de segurança da informação.

Uma vez quantificados os elementos básicos da análise de risco (Quadro 6), o modelo RACloud compõe um novo elemento – Evento (*E – Event*) – a partir da correlação dos elementos de ameaças e vulnerabilidades, ou seja, um evento de risco de segurança da informação é formado pela união de uma ameaça que explora uma determinada vulnerabilidade.

Este relacionamento entre ameaças e vulnerabilidades é estabelecido no modelo RACloud através de uma função de correlação de evento (α – *Alpha Function*). A função de correlação de evento faz uso dos níveis de risco e categorias de recurso (seção 3.2.1), além das propriedades de segurança (Quadro 5), para criar estratégias de correlação de exploração entre ameaças e vulnerabilidades.

A partir dos eventos de risco estabelecidos pela função de correção de evento são calculadas as probabilidades de ocorrência dos diversos eventos previamente correlacionados. O cálculo da probabilidade de ocorrência de determinado evento utiliza como base as variáveis DE e DD a partir das referências de elementos de ameaças (T) e vulnerabilidade (V) obtidas pela variável de evento (E) passada como parâmetro na função de probabilidade (*pf – Probability Function*). Da mesma forma como ocorre com as variáveis DD e DE, a variável de probabilidade (P) também é gerada de modo distinto para cada uma das propriedades de segurança da informação (Quadro 5) definidas pelo modelo RACloud.

O Quadro 10 apresenta a definição das variáveis de evento (E) e probabilidade (P) e das funções de correlação de evento e cálculo da probabilidade de um evento, que geram as variáveis E e P, respectivamente.

Quadro 10 – Definição de evento e probabilidade.

Símbolo	Descrição
$E_{T,V}$	**Event** que consiste na ameaça "T" explorar a vulnerabilidade "V"
$\alpha(T_{isl,rc,p[]}, V_{isl,rc,p[]})$	**Alpha Function** para correlação entre a ameaça "T" e a vulnerabilidade "V" $\alpha(T_{isl,rc,p[]}, V_{isl,rc,p[]}) = E_{T,V}$
$pf(E_{T,V}, CSP_y)$	**Probability Function** para determinado evento aplicado a determinado CSP
$P_{E,CSP,\{c,i,a\}}$	**Probability** de ocorrência do evento em determinado CSP para cada uma das propriedades de segurança da informação $pf(E_{T,V}, CSP_y) = \{P_{E,CSP,c}, P_{E,CSP,i}, P_{E,CSP,a}\}$

Finalmente, realizando a correlação entre eventos (E) e ativos de informação (A) o modelo RACloud chega na definição de risco. O elemento de risco (*R – Risk*) consiste na correlação de elementos de evento (E) que possuem potencial para impactar em propriedades de segurança da informação de elementos de ativos de informação (A). Para realizar tal correlação o modelo RACloud define a função de correlação de risco (*β - Beta Function*). Da mesma forma como ocorre com a função de correlação de evento (*α – Alpha Function*), a função de correlação de risco também faz uso dos níveis de risco e categorias de recurso (seção 3.2.1) para criar estratégias de correlação entre eventos e ativos de informação.

Uma vez estabelecido o correlacionamento entre eventos e ativos de informação, a função de risco (*rf – Risk Function*) do modelo RACloud faz o cálculo do risco de determinado cenário de risco (R) sobre determinado CSP. Para o cálculo do grau de risco (*DR – Degree of Risk*) a função de risco faz uso das variáveis P (*Probability*) e DI a partir das referências dos elementos E e A obtidos com base em R.

Conforme apresenta o Quadro 11 o grau de risco é gerado de modo distinto para cada uma das diferentes propriedades de segurança da informação. O Quadro 11 também apresenta a definição da variável de risco R (*Risk*) e das funções de correlação de risco e cálculo final do risco (*rf – Risk Function*).

Quadro 11 – Definição de risco e grau de risco.

Símbolo	Descrição
$R_{E,A}$	**Risk** que consiste no evento "E" gerar impacto sobre o ativo "A"
$\beta(E_{T,V}, A_{cc,ac})$	**Beta Function** para correlação entre o evento "E" e o ativo "A" $\beta(E_{T,V}, A_{cc,ac}) = R_{E,A}$
$rf(R_{E,A}, CSP_y)$	**Risk Function** para determinado risco aplicado a determinado CSP
$DR_{R,CSP,\{c,i,a\}}$	**Degree of Risk** Grau de risco do evento "E" em relação ao ativo "A" $rf(R_{E,A}, CSP_y) = \{DR_{R,CSP,c}, DR_{R,CSP,i}, DR_{R,CSP,a}\}$

É importante destacar que a determinação do tipo de análise a ser realizada, em relação aos tipos análise quantitativa ou análise qualitativa, ocorre pela forma como se especifica e implementa as funções de análise dos elementos de risco (`iaf()`, `daf()`, `eaf()`). Conforme explanado no início da seção 2.3.3, caso as funções de análise de risco sejam implementadas a partir de definições subjetivas para a quantificação das variáveis envolvidas no risco, então esta será uma análise qualitativa. Por outro lado, caso as funções possam se basear em dados históricos reais para a quantificação das variáveis envolvidas na análise de risco, neste caso a análise será quantitativa.

As definições de elementos, variáveis e funções apresentadas nesta seção são essenciais para o entendimento do modelo RACloud e servem de base para o desenvolvimento das próximas seções deste trabalho.

3.2.3 Funções de Correlação de Eventos e Riscos

Conforme apresentado no Quadro 10, a função de correlação de evento (α – *Alpha Function*) realiza a correlação entre elementos de ameaças e vulnerabilidades com o objetivo de formar eventos de incidentes de segurança da informação. Para tal correlação a função faz uso das informações de categoria de recurso (Quadro 2) e propriedade de segurança da informação (Quadro 5).

Uma determinada ameaça será correlacionada com uma determinada vulnerabilidade pela função de correlação de evento do modelo RACloud quando suas categorias de recursos forem iguais e pelo menos uma de suas propriedades de segurança for igual, ou seja, a ameaça deve explorar o mesmo recurso no qual a vulnerabilidade gera deficiência, e as propriedades de segurança visadas pela ameaça devem ser compatíveis com as propriedades de segurança fragilizadas pela vulnerabilidade. Neste caso considera-se que a ameaça tem potencial para explorar a vulnerabilidade, formando assim um evento potencial de incidente de segurança da informação.

O Quadro 12 apresenta uma matriz de correlação para a função de correlação de eventos (α – *Alpha Function*) do modelo RACloud. As linhas da matriz representam os 10 itens de RC (Quadro 2) possíveis para determinada ameaça, combinados com as 3 propriedades de segurança possíveis para cada item. As colunas da matriz representam os 10 itens de RC possíveis para determinada vulnerabilidade, também combinados com as 3 propriedade de segurança (Quadro 5).

Conforme demonstra o Quadro 12, uma ameaça será correlacionada com uma vulnerabilidade para a formação de um evento de incidente de segurança da informação quando os RCs de ambos forem iguais e quando pelo menos uma de suas propriedades de segurança for compatível.

Quando ao aspecto das propriedades de segurança, a ameaça será considerada correlacionada com a vulnerabilidade para todas as propriedades que estiverem ativas (forem válidas) para ambos os elementos.

Quadro 12 – Matriz de correlação entre ameaças e vulnerabilidades.

RC Threat X RC Vulnerability		Hardware			SO System			VM System			Communication System			Cloud System			Database			Framework			Application Server			Application System			Information System		
		C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A	C	I	A
Hardware	C	X																													
	I		X																												
	A			X																											
SO System	C				X																										
	I					X																									
	A						X																								
VM System	C							X																							
	I								X																						
	A									X																					
Communication System	C										X																				
	I											X																			
	A												X																		
Cloud System	C													X																	
	I														X																
	A															X															
Database	C																X														
	I																	X													
	A																		X												
Framework	C																			X											
	I																				X										
	A																					X									
Application Server	C																						X								
	I																							X							
	A																								X						
Application System	C																									X					
	I																										X				
	A																											X			
Information System	C																												X		
	I																													X	
	A																														X

Já a função de correlação de riscos (β - *Beta Function*), conforme apresentado no Quadro 11, faz a correlação entre elementos de eventos e elementos de ativos de informação, para formar cenários de risco de segurança da informação. Para realizar a correlação de cenários de risco a função de correlação de riscos faz uso das informações de RC de cada evento e AC (Quadro 3) de cada ativo de informação.

O Quadro 13 apresenta a matriz de correlação para a função de correlação de riscos (β - *Beta Function*) do modelo RACloud. As linhas

da matriz representam as RCs dos elementos de evento, enquanto as colunas representam as ACs dos elementos de ativos de informação. O símbolo “X” representam células que sempre se correlacionam, quando o símbolo “O” representam células que se correlacionam apenas quando o ativo de informação fizer uso do recurso em questão.

A RC Hardware, pertencente ao RL-0 (Hardware) se correlaciona com todas ACs de ativos de informação. Pelo fato da RC Hardware tratar de recursos muito básicos, como memória, CPU e disco, um evento nestes recursos impactaria em todas as categorias de ativos de informação. Pelo mesmo motivo, as RCs pertencentes ao RL-1 (Infraestrutura) também se correlacionam com todas as categorias de ativos de informação, quanto à formação de cenários de risco.

Quadro 13 – Matriz de correlação entre eventos e ativos de informação.

RL	Resource Category	Asset Category			
		File	Database	CC-Software	CSP-Software
0	Hardware	X	X	X	X
1	SO System	X	X	X	X
1	VM System	X	X	X	X
1	Communication System	X	X	X	X
1	Cloud System	X	X	X	X
2	Database		X	O	O
2	Framework			O	O
2	Application Server			O	O
3	Application System				O
3	Information System				O

Legenda – O: Opcionais.

A RC Database, pertencente ao RL-2 (Plataforma) se correlaciona com todos os ativos de informação da AC Database, além disto, correlaciona-se também com os ativos de informação das categorias CC-Software e CSP-Software, porém somente quando os softwares em

questão fazem uso da estrutura de banco de dados do CSP. Esta correlação se justifica pelo fato de que um evento de incidente de segurança da informação no recurso *database* impactaria nos ativos diretamente armazenados no Database, bem como em todos os softwares (do CC ou do CSP) que fazem uso das bases de dados do CSP.

Da mesma forma como ocorre com a RC Database, as RCs Framework e Application Server, do RL-2, também correlacionam-se com as categorias de ativos de informação CC-Software e CSP-Software, porém somente quando os softwares em questão fizerem uso da estrutura de framework ou servidor de aplicação do CSP, respectivamente.

As RCs do RL-3 (Software) correlacionam-se apenas com a categoria de ativos de informação CSP-Software. Estas RCs consideram apenas recursos de sistemas aplicativos e sistemas de informação do próprio CSP, impactando assim apenas em ativos de informação do CC diretamente acessado por softwares do CSP, ou seja, abrangendo apenas a AC CSP-Software. Esta correlação também se aplica somente quando o software em questão, onde estão as informações do CC, fizer uso dos recursos de sistemas aplicativos ou sistemas de informação do CSP.

3.3 RISK DEFINITION LANGUAGE

O modelo RACloud fornece uma linguagem para especificação de risco, a *RDL – Risk Definition Language*. A RDL é especificada em XML Schema (XSD) e contém informações sobre ameaças, vulnerabilidades e ativos de informação (seção 3.3.1). A RDL também define um XML específico para representação do resultado da análise de risco, o RDL de risco resultante (seção 3.3.2).

3.3.1 RDL de Elementos Básicos do Risco

A RDL permite a especificação de três tipos diferentes de registro: ativos de informação (Figura 12), ameaças (Figura 13) e vulnerabilidades (Figura 14).

Conforme descrevem as Figuras 9, 10 e 11, o cabeçalho da RDL para os três tipos (ameaças, vulnerabilidades e ativos de informação) é igual, contendo como atributos *type* e *id*; e como elementos os campos *source*, *version* e *description*, definidos conforme segue:

- *Type*: define o tipo de RDL, como CC, CSP ou ISL;
- *Id*: define o código interno do RDL para o CC, CSP ou ISL;

- *Source*: define o código do CC, CSP ou ISL para o modelo RACloud;
- *Version*: define a versão do RDL para o modelo RACloud;
- *Description*: apresenta uma descrição do propósito geral do RDL.

A definição RDL para ativos de informação (Figura 12) contém uma série de itens que descrevem os ativos de informação do CC a serem considerados na análise de risco no modelo RACloud. Cada item possui como atributo um identificador de item (*id*) e como elementos campos para descrição do item (*description*), categoria do ativo de informação (*category*) e quantificação do grau de impacto deste ativo em relação às propriedades de segurança da informação (*confidenciality, integrity e availability*).

Quando o ativo de informação for da categoria CC-Software ou CSP-Software, este poderá especificar um conjuntos de recursos (RCs – Resource Category) utilizados pelo software. Esta informação é especificada no campo *resources* que conterá um conjunto de elementos *resource*. Esta informação será utilizada no momento da execução da análise de risco, pela função de correlação de risco, para realizar a correlação entre eventos e ativos de informação (Quadro 13).

Figura 12 – Definição RDL para ativos de informação.

```
▼<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" attributeFormDefault="unqualified"
  ▼<xs:element name="RDL">
    ▼<xs:complexType>
      ▼<xs:sequence>
          <xs:element type="xs:string" name="source"/>
          <xs:element type="xs:string" name="version"/>
          <xs:element type="xs:string" name="description"/>
        ▼<xs:element name="informationAssets">
          ▼<xs:complexType>
            ▼<xs:sequence>
              ▼<xs:element name="item" maxOccurs="unbounded" minOccurs="0">
                ▼<xs:complexType>
                  ▼<xs:sequence>
                      <xs:element type="xs:string" name="description"/>
                      <xs:element type="xs:string" name="category"/>
                    ▼<xs:element name="resources" minOccurs="0">
                      ▼<xs:complexType>
                        ▼<xs:sequence>
                            <xs:element type="xs:string" name="resource" maxOccurs="unbounded"
                          </xs:sequence>
                        </xs:complexType>
                      </xs:element>
                      <xs:element type="xs:byte" name="confidenciality"/>
                      <xs:element type="xs:byte" name="integrity"/>
                      <xs:element type="xs:byte" name="availability"/>
                    </xs:sequence>
                    <xs:attribute type="xs:byte" name="id"/>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
        <xs:attribute type="xs:string" name="type"/>
        <xs:attribute type="xs:short" name="id"/>
      </xs:complexType>
    </xs:element>
  </xs:schema>
```

Fonte: Própria.

Para definição de uma ameaça o modelo RACloud especifica uma RDL de definição de ameaças conforme apresentado na Figura 13. Este RDL contém itens que representam ameaças a serem considerada na análise de risco de um ambiente de computação em nuvem. Os campos definidos para itens de uma ameaça são:

- *Description*: contém uma breve descrição da ameaça;
- *Type*: contém o tipo da ameaça, geralmente definido conforme tipos de ameaças constantes na ISO 27005;
- *Category*: define a categoria de recursos afetada por esta ameaça, conforme discutido previamente na seção 3.2.1;
- *WSRA* (*Web Service Risk Analysis*): define o endereço para o Web Service de análise de risco que fará a análise da ameaça em questão. Este Web Service irá implementar a função de análise de exposição e deverá retornar o grau de exposição (DE) da ameaça especificada neste item de RDL;

- *Reference*: contém uma referência externa para mais informações sobre a ameaça definida neste item de RDL. Geralmente faz referências para bases de ameaças como por exemplo o CVE ou NVT.

Figura 13 – Definição RDL para ameaças.

```
▼<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" attributeFormDefault="unqualified"
  ▼<xs:element name="RDL">
    ▼<xs:complexType>
      ▼<xs:sequence>
          <xs:element type="xs:string" name="source"/>
          <xs:element type="xs:float" name="version"/>
          <xs:element type="xs:string" name="description"/>
        ▼<xs:element name="threats">
          ▼<xs:complexType>
            ▼<xs:sequence>
              ▼<xs:element name="item" maxOccurs="unbounded" minOccurs="0">
                ▼<xs:complexType>
                  ▼<xs:sequence>
                      <xs:element type="xs:string" name="description"/>
                      <xs:element type="xs:string" name="type"/>
                      <xs:element type="xs:string" name="category"/>
                      <xs:element type="xs:anyURI" name="wsra"/>
                      <xs:element type="xs:string" name="reference"/>
                    </xs:sequence>
                    <xs:attribute type="xs:short" name="id"/>
                    <xs:attribute type="xs:string" name="propertyC"/>
                    <xs:attribute type="xs:string" name="propertyI"/>
                    <xs:attribute type="xs:string" name="propertyA"/>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
        <xs:attribute type="xs:string" name="type"/>
        <xs:attribute type="xs:short" name="id"/>
      </xs:complexType>
    </xs:element>
  </xs:schema>
```

Fonte: Própria.

Para realizar a correlação de eventos entre ameaças e vulnerabilidades, cada item de ameaça deve especificar quais propriedades de segurança da informação (Quadro 5) são afetadas por ele. Esta definição ocorre em 3 atributos específicos de definição das propriedades de segurança: *propertyC*, *propertyI, propertyA*.

A Figura 14 apresenta o XML Schema para um RDL de definição de vulnerabilidades no modelo RACloud. Este RDL possui a mesma estrutura de cabeçalho conforme já discutido no início desta seção. Quanto a estrutura de itens, o RDL de definição de vulnerabilidades é muito semelhante ao RDL de definição de ameaças. Possui os mesmos campos *description, type, category e WSRA,* com exceção do campo tipo, que não está presente no RDL de definição de vulnerabilidade, pois

neste caso o campo *category* já faz a função do campo de tipo de vulnerabilidade.

Da mesma forma como ocorre no RDL de definição de ameaças, no RDL de definição de vulnerabilidade o campo *category* também deve ser preenchido com uma categoria de recurso, conforme seção 3.2.1, e o campo WSRA deve endereçar um Web Service de análise de vulnerabilidade, que corresponde à função de análise de deficiência (*daf – deficiency analysis function*) que deve retornar o grau de deficiência (DD) da vulnerabilidade em questão. Os atributos *propertyC*, *propertyI, propertyA* devem especificar quais propriedades de segurança são fragilizadas pelo item de vulnerabilidade.

Figura 14 – Definição RDL para vulnerabilidades.

```
▼<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" attributeFormDefault="unqualified"
  ▼<xs:element name="RDL">
    ▼<xs:complexType>
      ▼<xs:sequence>
          <xs:element type="xs:string" name="source"/>
          <xs:element type="xs:float" name="version"/>
          <xs:element type="xs:string" name="description"/>
        ▼<xs:element name="vulnerabilities">
          ▼<xs:complexType>
            ▼<xs:sequence>
              ▼<xs:element name="item" maxOccurs="unbounded" minOccurs="0">
                ▼<xs:complexType>
                  ▼<xs:sequence>
                      <xs:element type="xs:string" name="description"/>
                      <xs:element type="xs:string" name="category"/>
                      <xs:element type="xs:anyURI" name="wsra"/>
                      <xs:element type="xs:string" name="reference"/>
                    </xs:sequence>
                    <xs:attribute type="xs:short" name="id"/>
                    <xs:attribute type="xs:string" name="propertyC"/>
                    <xs:attribute type="xs:string" name="propertyI"/>
                    <xs:attribute type="xs:string" name="propertyA"/>
                  </xs:complexType>
                </xs:element>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
        <xs:attribute type="xs:string" name="type"/>
        <xs:attribute type="xs:short" name="id"/>
      </xs:complexType>
    </xs:element>
  </xs:schema>
```

Fonte: Própria.

Exemplos da definição de RDLs de ativos de informação, ameaças e vulnerabilidades são apresentados no APÊNDICE D – RDLs DOS AGENTES CC E ISL, e serão discutidos no capítulo 4 onde será apresentado um protótipo do modelo RACloud.

3.3.2 RDL de Risco Resultante

A execução da análise de risco pelo modelo RACloud gera como resultado para o CC um registro RDL de risco resultante, com base na avalição do ambiente do CSP, considerando as ameaças e vulnerabilidades definidas pelo ISL e os impactos definidos pelo próprio CC.

O RDL de risco resultante está dividido em cabeçalho e riscos. A Figura 15 apresenta a especificação do cabeçalho do RDL de risco resultante do modelo RACloud.

Figura 15 – Cabeçalho da definição RDL de risco resultante.

```
▼<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" attributeFormDefault="unqualified"
  ▼<xs:element name="RDL">
    ▼<xs:complexType>
      ▼<xs:sequence>
          <xs:element type="xs:string" name="source"/>
          <xs:element type="xs:string" name="version"/>
          <xs:element type="xs:string" name="description"/>
          <xs:element type="xs:string" name="cc_id"/>
          <xs:element type="xs:string" name="csp_id"/>
        ▶<xs:element name="risks">...</xs:element>
        </xs:sequence>
        <xs:attribute type="xs:short" name="Id"/>
        <xs:attribute type="xs:string" name="type"/>
      </xs:complexType>
    </xs:element>
  </xs:schema>
```

Fonte: Própria.

O cabeçalho de RDL de risco resultante armazena informações como a origem a partir da qual o RDL foi gerado (source), a versão e uma descrição do RDL (version e description) e os Ids da entidades CC e CSP envolvidos na análise de risco (cc_id e csp_id).

O conjunto de elementos de risco (risks) resultantes da análise de risco está organizado em itens de risco (risk_item). Cada item de risco armazena as variáveis de risco calculado para os três requisitos de segurança considerados no modelo RACloud (DRa, DRc e DRi), além de um Id para o item de risco. Além de armazenar estas variáveis, cada item de risco também é formado por um elemento de ativo de informação (informationAsset) e um elemento de evento de segurança da informação (*event*). A Figura 16 apresenta a especificação do elemento informationAsset integrante do elemento risk_item, enquanto a Figura 17 apresenta a especificação do elemento *event*.

Figura 16 – Item de risco do RDL de risco resultante.

```
▼<xs:element name="risks">
  ▼<xs:complexType>
    ▼<xs:sequence>
      ▼<xs:element name="risk_item" maxOccurs="unbounded" minOccurs="0">
        ▼<xs:complexType>
          ▼<xs:sequence>
            ▼<xs:element name="informationAsset">
              ▼<xs:complexType>
                ▼<xs:simpleContent>
                  ▼<xs:extension base="xs:string">
                      <xs:attribute type="xs:byte" name="DIa" use="optional"/>
                      <xs:attribute type="xs:byte" name="DIc" use="optional"/>
                      <xs:attribute type="xs:byte" name="DIi" use="optional"/>
                      <xs:attribute type="xs:byte" name="id" use="optional"/>
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
            ▶<xs:element name="event">...</xs:element>
            </xs:sequence>
            <xs:attribute type="xs:byte" name="DRa" use="optional"/>
            <xs:attribute type="xs:byte" name="DRc" use="optional"/>
            <xs:attribute type="xs:byte" name="DRi" use="optional"/>
            <xs:attribute type="xs:byte" name="id" use="optional"/>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
```

Fonte: Própria.

Para cada item de risco o elemento de ativo de informação armazena as variáveis de impacto para as três propriedades de segurança da informação consideradas no modelo RACloud, além do Id e da descrição do ativo de informação em questão (conteúdo do elemento).

O elemento *event* é formado pelos elementos vulnerability e threat que representam a vulnerabilidade e a ameaça integrantes de cada item de risco, respectivamente. Conforme apresenta a Figura 17, tanto o elemento de vulnerabilidade quanto o de ameaça armazenam suas variáveis calculadas para cada propriedade de segurança (grau de deficiência e grau de exposição, respectivamente), além do Id da vulnerabilidade e ameaça e sua respectiva descrição, conteúdo do elemento. O elemento *event* também armazena as variáveis de probabilidade (Pa, Pc e Pi) para cada uma das propriedades de segurança, calculadas a partir das informações de vulnerabilidade e ameaça.

Figura 17 – Evento do RDL de risco resultante.

```
▼<xs:element name="event">
  ▼<xs:complexType>
    ▼<xs:sequence>
      ▼<xs:element name="vulnerability">
        ▼<xs:complexType>
          ▼<xs:simpleContent>
            ▼<xs:extension base="xs:string">
                <xs:attribute type="xs:byte" name="DDa" use="optional"/>
                <xs:attribute type="xs:byte" name="DDc" use="optional"/>
                <xs:attribute type="xs:byte" name="DDi" use="optional"/>
                <xs:attribute type="xs:short" name="id" use="optional"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      ▼<xs:element name="threat">
        ▼<xs:complexType>
          ▼<xs:simpleContent>
            ▼<xs:extension base="xs:string">
                <xs:attribute type="xs:byte" name="DEa" use="optional"/>
                <xs:attribute type="xs:byte" name="DEc" use="optional"/>
                <xs:attribute type="xs:byte" name="DEi" use="optional"/>
                <xs:attribute type="xs:short" name="id" use="optional"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute type="xs:byte" name="Pa" use="optional"/>
      <xs:attribute type="xs:byte" name="Pc" use="optional"/>
      <xs:attribute type="xs:byte" name="Pi" use="optional"/>
      <xs:attribute type="xs:string" name="id" use="optional"/>
    </xs:complexType>
  </xs:element>
```

Fonte: Própria.

Um exemplo de RDL de risco resultante é apresentado no apêndice E, resultado dos experimentos realizados a partir do protótipo do modelo RACloud, conforme Capítulo 5.

3.4 COMPONENTES DA ARQUITETURA

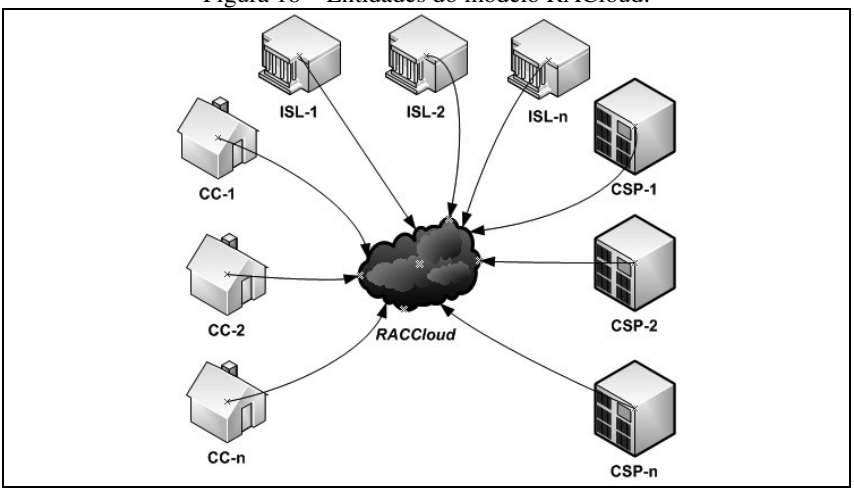
Esta seção apresenta os componentes arquiteturais do modelo RACloud e como estes componentes se relacionam durante a operacionalização do modelo, que está dividida em duas fases bem distintas: fase de especificação do risco e fase de análise do risco (SILVA, 2014 e SILVA, 2015).

3.4.1 Descrição dos Componentes

Conforme já introduzido anteriormente (seção 3.2.2), o modelo RACloud compartilha as responsabilidade pela definição e execução de uma análise de risco de segurança da informação entre três entidades principais – CC, CSP e ISL. A Figura 18 visa apresentar uma visão geral

do relacionamento das entidades CC, CSP e ISL com o modelo RACloud, onde é possível observar que o modelo prevê a participação de vários laboratórios ou grupos de segurança da informação (ISLs), atuando na análise de risco sobre vários ambientes de computação (CSPs) por solicitação de vários clientes de computação em nuvem (CCs).

Figura 18 – Entidades do modelo RACloud.



Fonte: Própria.

A arquitetura do modelo RACloud está organizada em três camadas: camada de agentes (*Agent Layer*), camada de conexão (*Conn Layer*) e camada de núcleo (*Core Layer*), conforme ilustrado na Figura 19.

A camada mais alta do modelo (*Agent Layer*) situa-se distribuída entre os ambientes de tecnologia das entidades CC, CSP e ISL, enquanto que as camadas *Conn Layer* e *Core Layer* situam-se no próprio ambiente de tecnologia que hospeda o RACloud. Este ambiente pode pertencer a um ISL específico ou qualquer outra entidade que tenha por objetivo administrar RACloud. Esta entidade será nomeada no modelo RACloud como *RAP – Risk Analysis Provider*.

A entidade RAP tem por responsabilidade hospedar as camadas de conexão e núcleo do modelo, formadas pelos componentes Conn ISL, Conn CC, Conn CSP, Agent Manager, RDL Manager e Analysis Manager.

Os componentes Conn ISL, Conn CC e Conn CSP são interfaces para comunicação com outros componentes distribuídos, respectivamente, entre as entidades ISL, CC e CSP na *Agent Layer*.

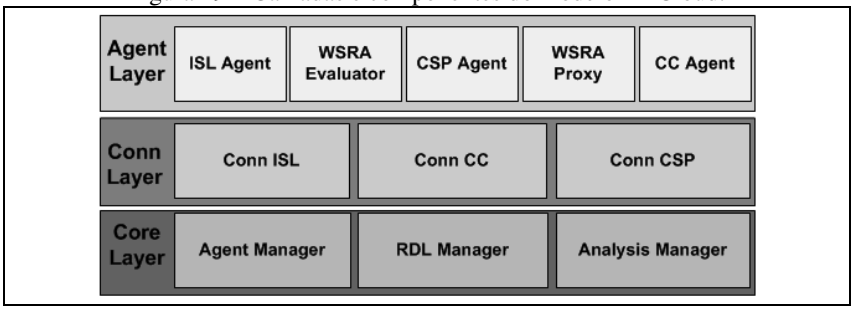
O componente Agent Manager é responsável por gerenciar o registro das entidades CC, CSP e ISL no modelo RACloud. O componente RDL Manager é responsável por gerenciar e armazenar os registros de definição de riscos, ou seja, os RDLs de definição de ativos de informação, ameaças e vulnerabilidades. E o componente Analysis Manager é responsável por realizar a correlação dos eventos e riscos e o cálculo final do risco.

A entidade ISL representa um laboratório ou grupo especializado em segurança da informação, sua responsabilidade é especificar os RDLs de vulnerabilidades e ameaças, além dos respectivos WSRAs de análise das vulnerabilidades e ameaças. Esta entidade hospeda os componentes ISL Agent e WSRA Evaluator.

O componente ISL Agent é responsável por registrar o ISL no Agent Manager e publicar suas RDLs de definição de ameaças e vulnerabilidades no RDL Manager.

O componente WSRA Evaluator é responsável por realizar as análises das ameaças e vulnerabilidades descritas nos RDLs. Este componente implementa as funções de análise de ameaças e vulnerabilidades as quais retornam, respectivamente, as variáveis de grau de exposição (DE) e grau de deficiência (DD) para as três propriedades de segurança da informação definidas no modelo RACloud.

Figura 19 – Camadas e componentes do modelo RACloud.



Fonte: Própria.

A entidade CSP representa o próprio *cloud service provider* alvo da análise de risco. Esta entidade hospeda os componentes CSP Agent e WSRA Proxy.

O componente CSP Agent é responsável por registrar o CSP no Agent Manager e inscrever-se nas RDLs em que o CSP deseja ser analisado. Enquanto que o componente WSRA Proxy é responsável por coletar informações do CSP e realizar a chamada do WSRA Evaluator de modo que o ISL possa realizar a análise de ameaças e vulnerabilidades no ambiente do CSP.

A entidade CC representa o cliente do CSP, que hospeda seus ativos de informação na nuvem e deseja conhecer o risco ao qual está sujeito em relação a seu CSP. Esta entidade hospeda o componente CC Agent. Este componente é responsável por registrar o CC no RACloud, disponibilizar as RDLs de ativos de informação do CC e iniciar a análise de risco comunicando-se com o componente Analysis Manager através do componente Conn CC.

Os componentes da arquitetura do modelo RACloud possuem diferentes responsabilidades nas fases de especificação do risco e análise do risco. As duas próximas seções detalham cada uma destas fases respectivamente.

3.4.2 Fase de Especificação do Risco

A fase de especificação do risco é o momento em que são definidas as vulnerabilidades, ameaças e ativos de informação que farão parte da análise de risco. Nesta fase também são definidas a função de análise de exposição para cada ameaça e a função de análise de deficiência para cada vulnerabilidade.

Inicialmente as entidades ISL (uma ou várias) definem as ameaças e vulnerabilidades que desejam fornecer ao modelo RACloud para a realização de uma análise de risco. Esta definição consiste na especificação de elementos T e V conforme definidos no Quadro 6. Estes elementos básicos de risco serão especificados pelos ISLs na forma de um ou vários RDLs de ameaças e vulnerabilidades, conforme definido nas Figura 13 e 11, respectivamente.

Uma vez especificados os RDLs de ameaças e vulnerabilidades, as entidades ISL também precisam especificar, implementar e fornecer as funções WSRA para análise de exposição e deficiência. A função de análise de exposição ($eaf(T_{isl,rc}, CSP_y)$) será especificada no campo WSRA de cada item de RDL de ameaça (Figura 13) e deverá

retornar o grau de exposição ($DE_{T,CSP,\{c,i,a\}}$) para cada uma das propriedades de segurança da informação, conforme especificado no Quadro 9. Da mesma forma, a função de análise de deficiência ($daf(V_{isl,rc}, CSP_y)$) será especificada no campo WSRA de cada item de RDL de vulnerabilidade (Figura 14) e deverá retornar o grau de deficiência ($DD_{V,CSP,\{c,i,a\}}$) para cada uma das propriedades de segurança da informação, conforme especificado no Quadro 8.

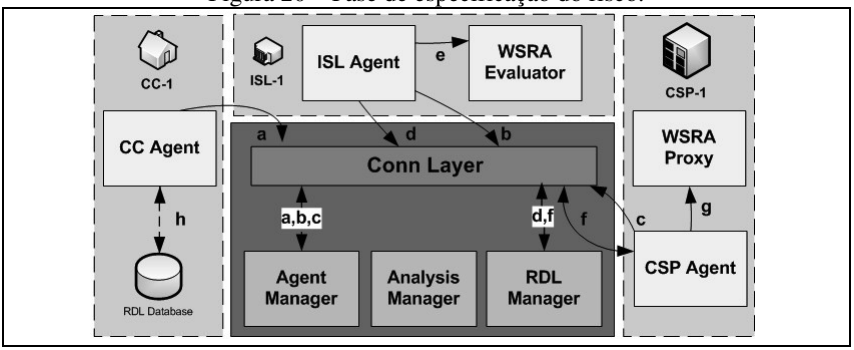
As entidades CSP tem por responsabilidade na fase de especificação do risco implementar e fornecer suas interfaces WSRA Proxy. Cada interface WSRA Proxy do CSP deve corresponder a uma função WSRA de uma ameaça ou vulnerabilidade para a qual o CSP deseja ser analisado, e deverá ser implementada pelo CSP de modo a atender aos objetivos e necessidades de sua respectiva ameaça ou vulnerabilidade.

Cada entidade CC participante de uma análise de risco no modelo RACloud deve, na fase de especificação do risco, definir seus RDLs de ativos de informação, conforme definido na Figura 12. Cada item de um RDL de ativos de informação corresponde a um elemento A (Quadro 6) da análise de risco e deve fornecer o grau de impacto ($DI_{A,\{c,i,a\}}$) para cada uma das propriedades de segurança da informação, conforme Quadro 7. Quanto a função de análise de impacto ($iaf(A_{cc,ac})$), esta não é implementada e fornecida pela entidade CC, mas sim pelo próprio modelo RACloud, na figura do componente Analysis Manager.

A Figura 20 ilustra a distribuição dos componentes do modelo RACloud entre as entidades CC, CSP e ISL, e o fluxo de interações entre estes componentes durante a fase de especificação do risco.

Inicialmente os componentes CC, CSP e ISL Agent, localizados respectivamente nas entidades CC, CSP e ISL devem registra-se no componente Agent Manager através das interfaces fornecidas pela camada de conexão (Figura 20 a, b, c). Então o ISL Agent registrar suas RDLs no componente RDL Manager (Figura 20 d) e publica suas funções de análise de ameaças e vulnerabilidades no componente WSRA Evaluator (Figura 20 e).

Figura 20 – Fase de especificação do risco.



Fonte: Própria.

A atuação da entidade CSP na fase de especificação do risco consiste em importar os RDLs registrados pelo ISL no componente RDL Manager (Figura 20 f), implementar os WSRAs Proxy e publicá-los no componente WSRA Proxy (Figura 20 g).

A atuação da entidade CC na fase de especificação do risco consiste apenas em armazenar seus RDLs de ativos de informação na base de dados de RDLs do componente CC Agent (Figura 20 h).

Uma vez definidos os elementos para ameaças, vulnerabilidades e ativos de informação, e registradas as entidades CC, CSP e ISL participantes da análise de risco, o modelo RACloud está pronto para a fase de análise de risco.

3.4.3 Fase de Análise do Risco

Na fase de análise do risco ocorre a execução das funções de análise de impacto, exposição e deficiência para cada um dos elementos de ativos de informação, ameaças e vulnerabilidades especificados pelos RDLs das entidades CC e ISL participantes da análise de risco.

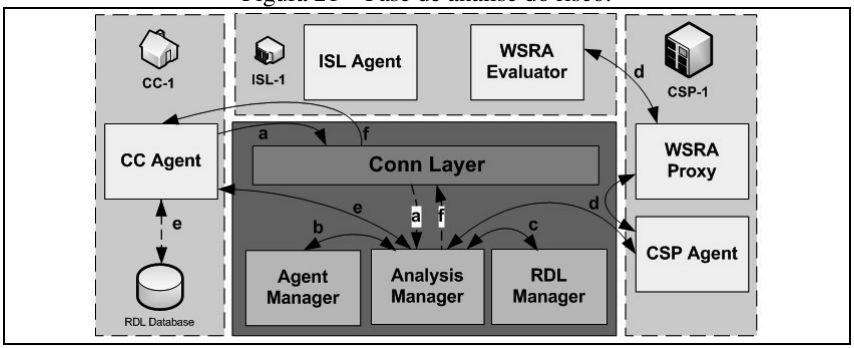
Como resultado da execução destas funções, tem-se a quantificação das variáveis de grau de impacto ($DI_{A,\{c,i,a\}}$), grau de exposição ($DE_{T,CSP,\{c,i,a\}}$) e grau de deficiência ($DD_{V,CSP,\{c,i,a\}}$) para cada uma das propriedades de segurança da informação.

Uma vez analisados os elementos básicos do risco (Quadro 6), ocorre nesta fase a geração dos eventos de risco ($E_{T,V}$) através da chamada da função de correlação de eventos ($\alpha(T_{isl,rc}, V_{isl,rc})$). E a partir dos eventos resultantes da função de correlação de eventos,

calcula-se a probabilidade de um evento ocorrer ($P_{E,CSP,\{c,i,a\}}$), através da função de probabilidade ($pf(E_{T,V}, CSP_y)$), conforme especificado pelo Quadro 10, seção 3.2.2.

A última parte da fase de análise do risco consiste na definição dos elementos de risco e no cálculo final do grau de risco. A definição dos elementos de risco ($R_{E,A}$) ocorre através da correlação de elementos de eventos ($E_{T,V}$) com elementos de ativos de informação ($A_{cc,ac}$), pela chamada da função de correlação de risco ($\beta(E_{T,V}, A_{cc,ac})$). Finalmente, na fase de análise do risco, calcula-se o grau de risco ($DR_{R,CSP,\{c,i,a\}}$) para cada uma das propriedades de segurança da informação em cada um dos elementos de risco, através da chamada da função de risco ($rf(R_{E,A}, CSP_y)$), conforme especificado pelo Quadro 11, seção 3.2.2.

Figura 21 – Fase de análise do risco.



Fonte: Própria.

A Figura 21 ilustra o fluxo de interações entre as entidades CC, CSP e ISL durante a fase de análise do risco. A análise do risco inicia com o componente CC Agent informando o CSP que será analisado (Figura 21 a). A partir disto o componente Analysis Manager verifica se o CSP em questão está registrado e obtém suas informações, consultando o componente Agent Manager (Figura 21 b). O componente Analysis Manager também obtém os RDLs registrados, consultando o componente RDL Manager (Figura 21 c).

De posse das informações sobre o CSP e os RDLs registrados, o componente Analysis Manager inicia a análise das ameaças e vulnerabilidades, invocando o componente CSP Agent. No CSP ocorre a chamada dos WSRAs Proxy que farão a análise local da respectiva ameaça ou vulnerabilidade e enviarão estas informações para o WSRA

do ISL no componente WSRA Evaluator, onde ocorre a quantificação da variável de grau de exposição ou grau de deficiência. O resultado da análise do WSRA Evaluator retorna então para o Analysis Manager, via WSRA Proxy e CSP Agent (Figura 21 d).

Após quantificar todas as ameaças e vulnerabilidades definidas nos RDLs registrados, inicia-se a quantificação dos impactos definidos pela entidade CC. Para tanto, o componente Analysis Manager invoca o componente CC Agent para obter o grau de impacto de seus ativos de informação. O componente CC Agent consulta o grau de impacto de seus ativos de informação para cada uma das propriedades de segurança e retorna esta informação para o componente Analysis Manager (Figura 21 e).

Uma vez obtidas todas as quantificações das variáveis relativas aos elementos básicos de risco, o componente Analysis Manager invoca internamente suas funções de correlação de eventos para a geração dos elementos de eventos, e correlação de riscos para a geração dos elementos de riscos. Finalmente, são calculados a probabilidade de cada elemento de evento e o grau de risco de cada elemento de risco.

O resultado da análise do risco é então retornado para o CC na forma de um RDL de risco resultante (Figura 15), para que este faça então sua avaliação quanto a aceitação ou não dos riscos encontrados em seu CSP (Figura 21 f).

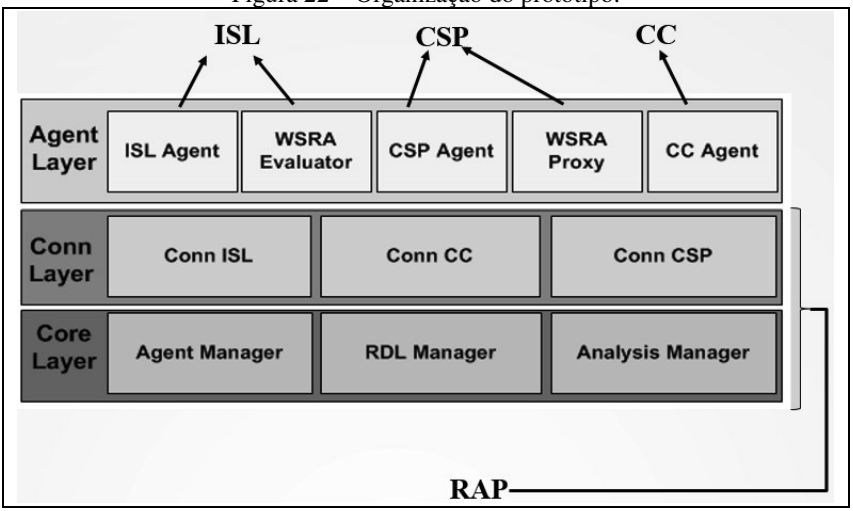
4 PROTÓTIPO DO MODELO RACLOUD

A partir do modelo proposto, foi especificado e implementado um protótipo para a realização de experimentos da modelagem de risco, linguagem de definição de risco e componentes da arquitetura. A primeira seção deste capítulo descreve a organização deste protótipo em seis diferentes projetos. As seis seções seguintes (4.2 à 4.7) descrevem em detalhes cada um dos projetos integrantes do protótipo RACloud.

4.1 ORGANIZAÇÃO DO PROTÓTIPO

O protótipo do modelo RACloud é composto por seis projetos distintos os quais representam os diferentes componente do modelo. A organização dos componentes do protótipo em relação às entidades participantes da análise de risco é apresentada na Figura 22.

Figura 22 – Organização do protótipo.



Fonte: Própria.

Os projetos integrantes do protótipo do modelo RACloud são:

- **RACloud-Prototype**: representa as camadas Core Layer e Conn Layer do modelo RACloud, incluindo os componentes Agent Manager, RDL Manager e Analysis Manager, além dos componentes de conexão para ISL, CC e CSP conforme

descritos anteriormente. Este projeto é especificado, implementado, alocado e executado pela entidade provedora do RACloud (entidade RAP – *Risk Analysis Provider*). Esta entidade pode ser um ISL específico ou qualquer outra instituição independente;

- **RACloud-CC-Agent**: representa o componente CC Agent da camada Agent Layer. Este projeto corresponde a parte do protótipo alocada e executada sob responsabilidade do CC, porém especificada e implementada pelo RAP;
- **RACloud-ISL-Agent**: representa o componente ISL Agent da camada Agent Layer. Este projeto corresponde a parte do protótipo alocada e executada sob responsabilidade de um ISL, porém especificada e implementada pelo RAP;
- **RACloud-CSP-Agent**: representa o componente CSP Agent da camada Agent Layer. Este projeto corresponde a parte do protótipo alocada e executada sob responsabilidade do CSP que terá seu ambiente tecnológico de nuvem analisado, porém, como ocorre com os outros agentes, especificada e implementada pelo RAP;
- **RACloud-CSP-WSRA-Proxy**: representa o componente WSRA Proxy da camada Agent Layer. Este projeto é especificado, implementado, alocado e executado pelo CSP, diferentemente do que o ocorre com o projeto RACloud-CSP-Agent que é apenas alocado e executado pelo CSP, ou seja;
- **RACloud-ISL-WSRA-Evaluator**: corresponde ao componente WSRA Evaluator da camada Agent Layer. Este projeto é especificado, implementado, alocado e executado pelo ISL, diferentemente do que ocorre com o projeto RACloud-ISL-Agent que é apenas alocado e executado pelo ISL.

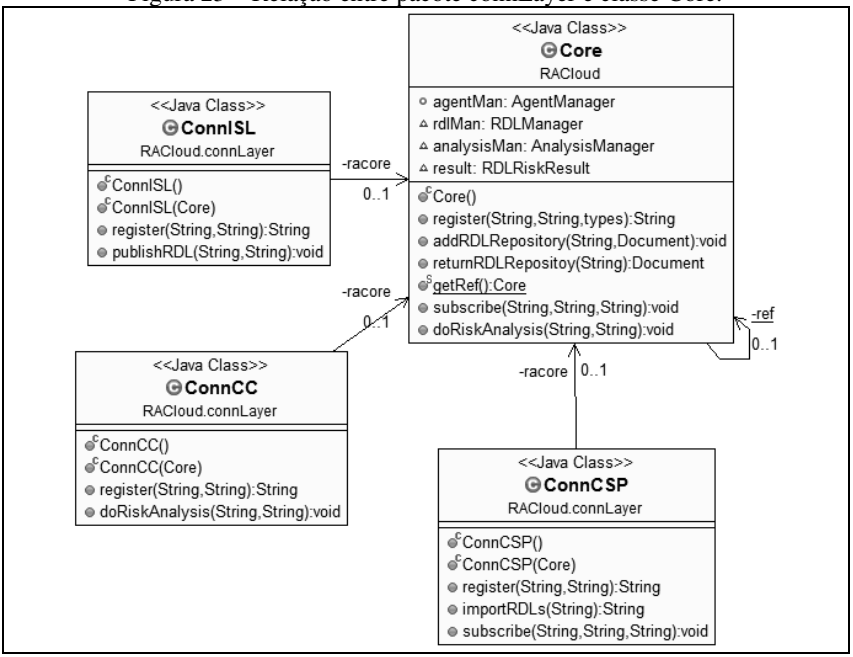
4.2 PROJETO RACLOUD-PROTOTYPE

A especificação do projeto RACloud-Prototype define um pacote chamado RACloud e três outros pacotes interno ao pacote RACloud: connLayer, elements e rdlManager. Estes quatro pacotes são especificados conforme os diagramas de classes das figuras 21 à 25.

A Figura 23 apresenta a relação entre as classes do pacote connLayer e a classe principal do protótipo, classe Core. As classes

ConnISL, ConnCC e ConnCSP são interfaces para os agentes ISL, CC e CSP respectivamente. Através destas classes os agentes inicialmente se registram no protótipo RACloud (método register).

Figura 23 – Relação entre pacote connLayer e classe Core.

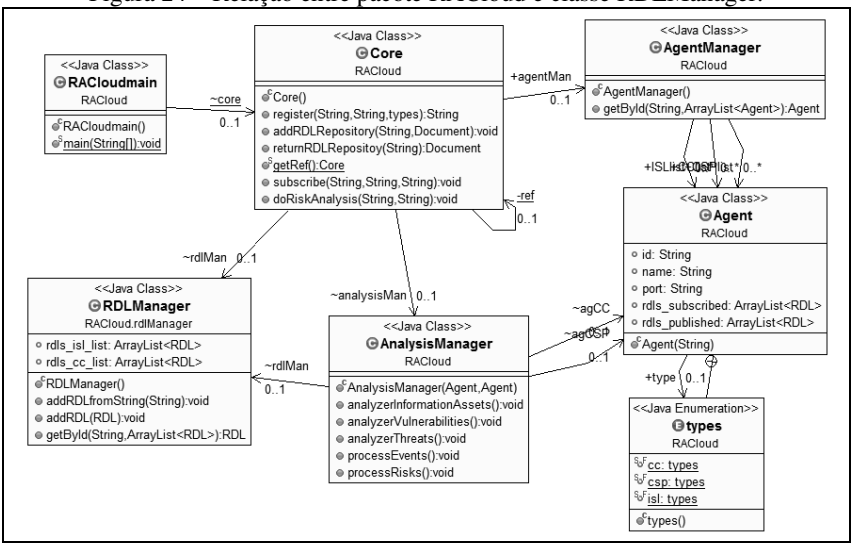


Fonte: Própria.

Feito o registro dos agentes, a classe ConnISL permite ao ISL publicar seus RDLs (método publishRDL), enquanto que a classe ConnCSP permite ao CSP assinar e importar os RDLs de seu interesse. Já a classe ConnCC permite ao CC exportar seus RDLs (método exportRDL) e iniciar a análise de risco (método doRiskAnalysis).

Todas as informações recebidas pelo protótipo através da camada de conexão chegam à classe Core, que tem por objetivo gerenciar o protótipo e coordenar a fase de especificação e análise de risco.

Figura 24 – Relação entre pacote RACloud e classe RDLManager.



Fonte: Própria.

A Figura 24 apresenta as classes do pacote RACloud e sua relação com a classe RDLManager do pacote rdlManager. Este pacote possui uma classe principal apenas para iniciar o projeto (classe RACloudmain) e a classe Core, que tem por objetivo gerenciar toda a execução do protótipo.

A classe Core recebe dos agente externos CC, CSP e ISL, via camada de conexão, (i) o registro deste agentes no protótipo; (ii) os RDLs de CC e ISL; e (iii) a assinatura do CSP aos RDLs que ele deseja implementar.

Os registros dos agentes CC, CSP e ISL são passados pela classe Core para a classe AgentManager, que faz a instanciação dos agentes no protótipo (classe Agent) e o gerenciamento destes agentes. A enumeração types define o tipo de agentes possíveis de serem instanciados no modelo RACloud, conforme definição do Quadro 4.

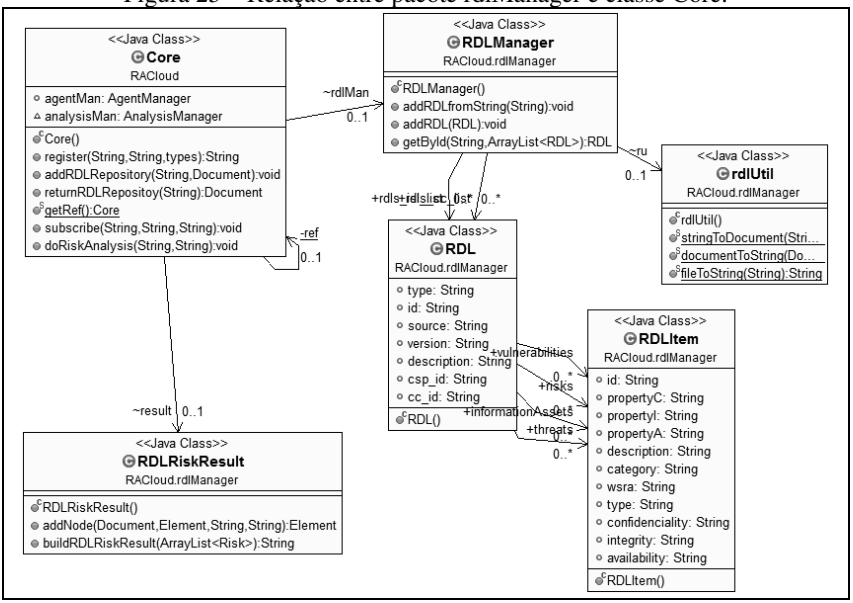
As informações de RDLs recebidas pela classe Core dos agentes CC e ISL são encaminhadas para a classe RDLManager do pacote RDL, para armazenamento e gerenciamento. As solicitações dos CSPs para implementarem um ou vários RDLs também são encaminhadas para a classe RDLManager para que esta retorne os RDLs ao CSP.

A classe Core também é responsável por receber do CC a solicitação para iniciar a análise de risco (método doRiskAnalysis). Esta

solicitação inicia uma classe AnalysisManager que irá interagir com os Agentes e RDLs para a execução da análise de risco e o retorno dos resultados ao CC solicitante.

A Figura 25 apresenta as classes do pacote rdlManager e sua relação com a classe Core do pacote RACloud. Um vez que a classe RDLManager recebe um RDL da classe Core (vindo de um CC ou ISL), ela faz uso da classe rdlUtil para conversões de formato do RDL, quando necessário. As classes RDL e RDLItem são instanciadas pela classe RDLManager para armazenamento e gerenciamento dos RDLs recebidos.

Figura 25 – Relação entre pacote rdlManager e classe Core.



Fonte: Própria.

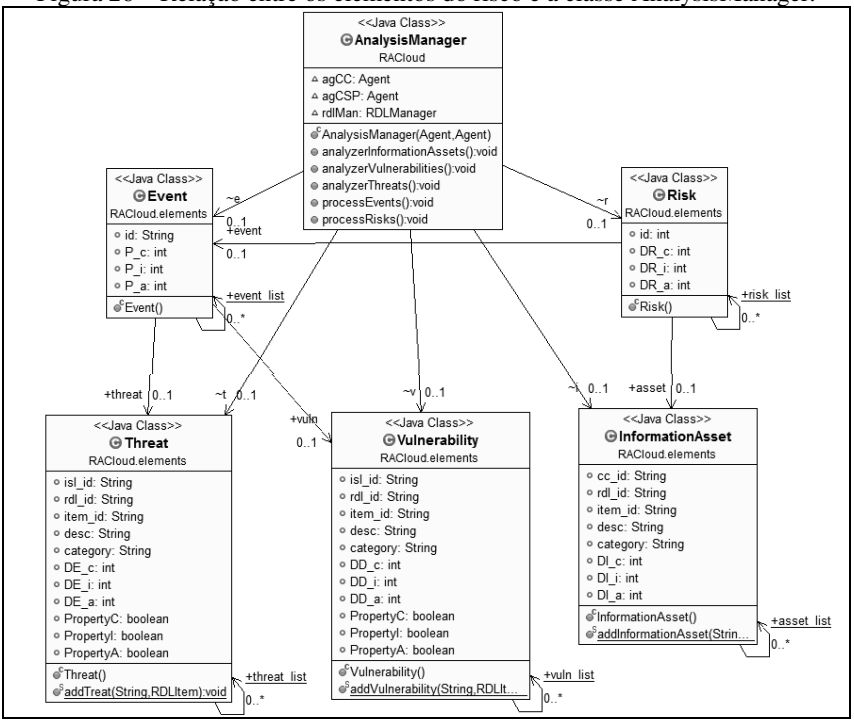
No pacote rdlManager a classe Core também relaciona-se com a classe RDLRiskResult. A classe RDLRiskResult é responsável por montar o RDL de resultado de risco que será retornado para o CC pela classe Core após a execução da análise de risco (pelo método doRiskAnalysis).

Durante a execução da análise de risco a classe AnalysisManager faz a análise de todos os elementos integrantes do risco. A Figura 26 apresenta a relação da classe AnalysisManager do pacote RACloud com

as classes que representam os elementos integrante do risco, no pacote elements.

Inicialmente a classe AnalysisManager faz a análise dos elementos básicos da análise de risco (conforme Quadro 6). O método analyzerInformationAssets é responsável pela análise do grau de impacto dos ativos de informação, conforme Quadro 7 da modelagem do risco. Da mesma forma os métodos analyzerVulnerabilities e analyzerThreats são responsáveis pela análise dos graus de deficiência e exposição, conforme Quadro 8 e Quadro 9 da modelagem do risco, respectivamente. Para tanto, a classe AnalysisManager relaciona-se com as classes InformationAsset, Vulnerability e Threat.

Figura 26 – Relação entre os elementos do risco e a classe AnalysisManager.

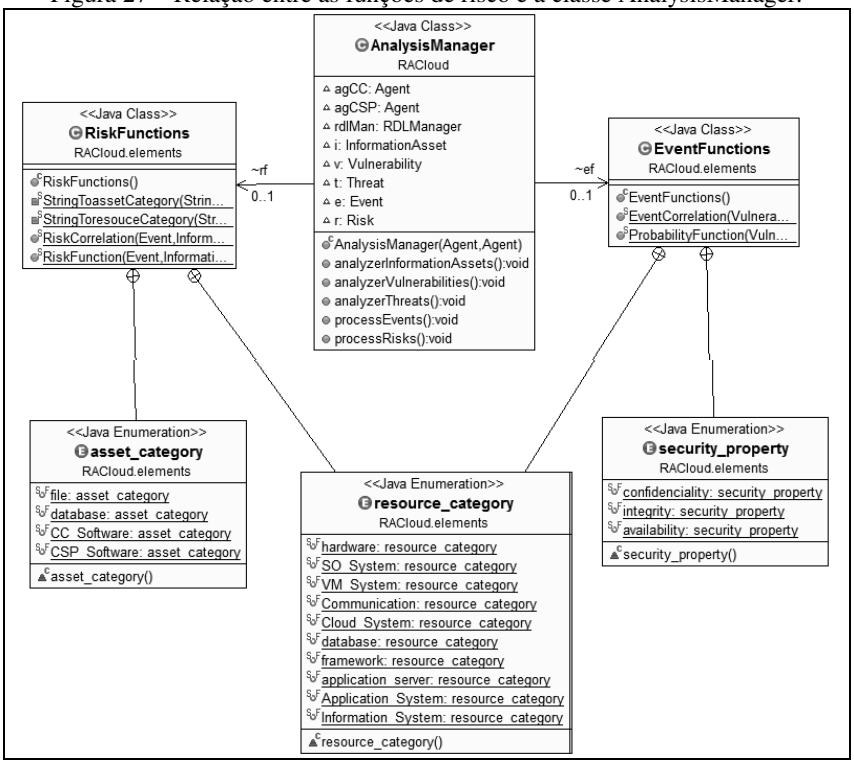


Fonte: Própria.

Após a análise dos elementos básicos do risco, a classe AnalysisManager realiza o processamento dos eventos (método processEvents) e dos riscos (método processRisks), para tal, a classe AnalysisManager relaciona-se com as classes Event e Risk do pacote elements.

Ainda analisando o relacionamento entre as classes de elementos de risco, observa-se que a classe Event relaciona-se com as classes Threat e Vulnerability, e a classe Risk relaciona-se com a classe Event e InformationAsset, seguindo as definições especificadas conforme Quadro 10 e Quadro 11 para eventos e riscos, respectivamente.

Figura 27 – Relação entre as funções de risco e a classe AnalysisManager.



Fonte: Própria.

No projeto RACloud-Prototype foram definidas duas classes específicas para representarem as funções relacionadas com eventos e riscos (Figura 27). A classe EventFunctions define as funções de correlação de eventos e cálculo de probabilidade, conforme Quadro 10 da modelagem do risco. Esta classe é chamada pela classe AnalysisManager no momento do processamento dos eventos (método processEvents). A classe RiskFuncions define as funções de correlação de riscos e cálculo do grau de risco, conforme Quadro 11 da modelagem

do risco. Esta classe é chamada pela classe AnalysisManager no momento do processamento dos riscos (método processRisks).

Para realizar a correlação de eventos de incidentes de segurança da informação a classe EventFunctions faz uso das enumerações resource_category e asset_category, que representam as definições RC (Quadro 2) e AC (Quadro 3) do modelo RACloud, respectivamente. Estas duas enumerações são utilizadas pela classe EventFunctions para implementar a função de correlação de eventos (α – *Alpha Function*) conforme descrito na seção 3.2.3 (Quadro 12).

A função de cálculo de probabilidade (função *pf* do Quadro 10) faz uma validação de quais propriedades de segurança são válidas para o evento em questão e realiza uma média aritmética simples entre DD e DE apenas para estas propriedades de segurança, resultando nas variáveis $P_{E,CSP,\{c,i,a\}}$ apenas para as propriedades de segurança da informação válidas.

Para realizar a correlação de cenários de riscos de segurança da informação a classe RiskFunction faz uso das enumerações resource_category e security_property (Quadro 5). Estas duas enumerações são utilizadas pela classe RiskFunctions para implementar a função de correlação de riscos (β - *Beta Function*) conforme descrito na seção 3.2.3 (Quadro 13).

A função de cálculo de risco (função *rf* do Quadro 11) faz uma validação das propriedades de segurança ativas no evento em questão e realiza uma média aritmética simples entre P e DI apenas para as propriedades ativas (previamente calculadas na função *pf*), resultado nas variáveis $DR_{R,CSP,\{c,i,a\}}$ apenas para estas propriedades.

4.3 PROJETO RACLOUD-CC-AGENT

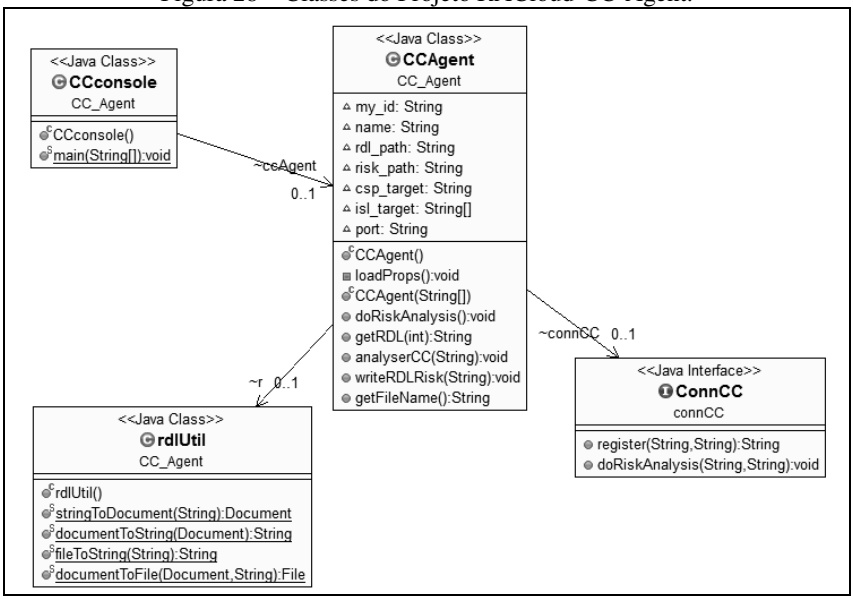
O projeto RACloud-CC-Agent possui três classes principais: CCconsole, CCAgent e rdlUtil, além de uma interface: ConnCC (Figura 28). A classe CCconsole representa o console de comandos executado pelo CC a partir do qual ele realiza os comandos de interação com o modelo RACloud. O principal comando executado pelo CC através do console é o comando doRiskAnalysis, que inicia a execução de uma análise de risco.

A classe CCAgent representa o componente CC Agent (Figura 19) da arquitetura RACloud. Esta classe faz invocações aos métodos da interface ConnCC para comunicação com o projeto RACloud-Prototype,

e também fornece métodos a serem invocados pelo RACloud-Prototype durante a execução da análise de risco.

Inicialmente a classe CCAgent lê o arquivo de configuração do agente (método loadProps), faz o registro do CC no modelo RACloud (método register) e aguarda comandos do CCconsole. Ao receber o comado para iniciar a análise de risco (método doRiskAnalysis) a classe CCAgent repassa este comando para a interface ConnCC e aguarda solicitações do RACloud-Prototype.

Figura 28 – Classes do Projeto RACloud-CC-Agent.



Fonte: Própria.

Durante a execução da análise de risco o RACloud-Prototype consulta as RDLs do CCAgent, através da invocação do método getRDL, para obtenção de informações sobre os ativos de informação especificados pelo CC.

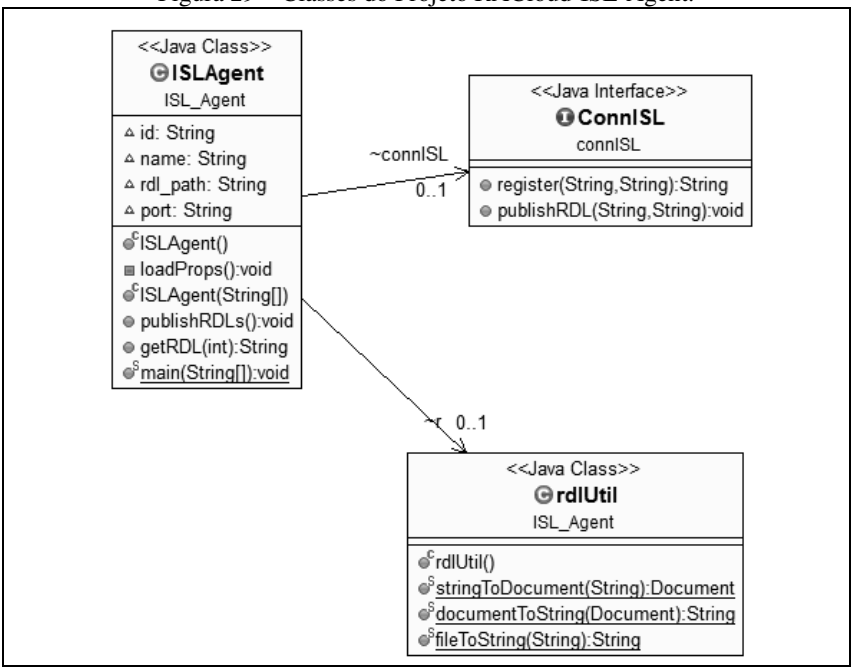
Ao final da análise de risco o RACloud-Prototype repasse ao CCAgent o RDL de risco resultante, através do método writeRDLRisk. Desta forma o CC recebe o resultado da análise de risco.

Para transformações e manipulações das RDLs, o projeto RACloud-CC-Agent faz uso da classe rdlUtil.

4.4 PROJETO RACLOUD-ISL-AGENT

O projeto RACloud-ISL-Agent possui duas classes principais: ISLAgent e rdlUtil, e uma interface: ConnISL (Figura 29). Da mesma forma como ocorre no projeto RACloud-CC-Agent, a classe rdlUtil é usada para manipulações e transformações nos RDLs, e a interface ConnISL é usada para comunicação com o projeto RACloud-Prototype.

Figura 29 – Classes do Projeto RACloud-ISL-Agent.



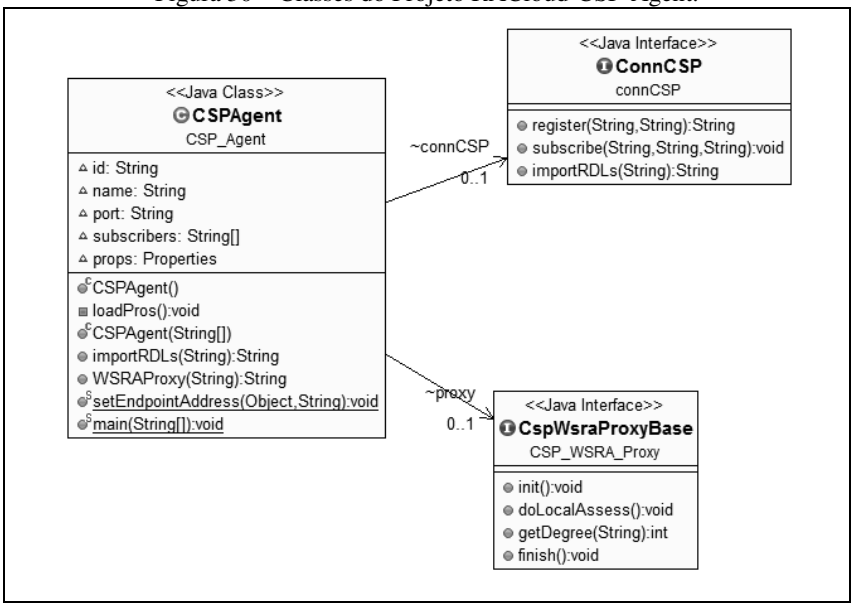
Fonte: Própria.

A classe ISLAgent inicialmente faz a leitura do arquivo de configuração do agente (método loadProps) e registra o agente no RACloud-Prototype, via método register da interface ISLConn. Em seguida, com base nas informações contidas no arquivo de configuração, a classe ISLAgent publica seus RDLs de ameaças e vulnerabilidades junto ao RACloud-Prototype (método publishRDL).

4.5 PROJETO RACLOUD-CSP-AGENT

O projeto RACloud-CSP-Agent possui uma classe principal, CSPAgent, e duas interfaces: ConnCSP e CspWsraProxyBase (Figura 30). A interface ConnCSP é usada para comunicação com o projeto RACloud-Prototype, enquanto que a interface CspWrsaProxyBase é usada para comunicação com o projeto RACloud-CSP-WSRA-Proxy.

Figura 30 – Classes do Projeto RACloud-CSP-Agent.



Fonte: Própria.

Da mesma forma como ocorre com as classes CCAgent e ISLAgent, dos projetos RACloud-CC-Agent e RACloud-ISL-Agent, a classe CSPAgent inicialmente faz a leitura de seu arquivo de configuração e o registro do agente no RACloud-Prototype.

Posteriormente, com base nas informações do arquivo de configuração, definidas pelo CSP, a classe CSPAgent se inscreve (método subscribe) nas RDLs de ameaças e vulnerabilidades em que deseja ser analisada quando aos riscos de segurança da informação.

A interface CspWsraProxyBase representa um ponto de comunicação para um WSRAProxy do projeto RACloud-CSP-WSRA-Proxy. Esta interface gera um WSDL para ser importado pelo projeto RACloud-CSP-WSRA-Proxy, conforme especificado na Figura 31,

onde um WSRA Proxy deve possuir métodos para sua inicialização (método init) e finalização (método finish), além de métodos para a execução da avaliação (doLocalAssess) e para a consulta do grau de exposição ou deficiência resultante da avaliação (getDegree).

Figura 31 – Definição WSDL para WSRA-Proxy.

```
▼<definitions xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsp="http://www.
  xmlns:wsp1_2="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata" xmlns:soap=
  xmlns:tns="http://CSP_WSRA_Proxy/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.xmlsoap.org/wsdl/" targetNam
  name="csp_wsra_proxy_baseService">
  ▼<types>
    ▶<xsd:schema>...</xsd:schema>
    </types>
  ▶<message name="init">...</message>
  ▶<message name="initResponse">...</message>
  ▶<message name="doLocalAssess">...</message>
  ▶<message name="doLocalAssessResponse">...</message>
  ▶<message name="getDegree">...</message>
  ▶<message name="getDegreeResponse">...</message>
  ▶<message name="finish">...</message>
  ▶<message name="finishResponse">...</message>
  ▼<portType name="csp_wsra_proxy_base">
    ▼<operation name="init">
       <input wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/initRequest" message="tns:init"/>
       <output wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/initResponse" message="tns:initResponse"/>
     </operation>
    ▼<operation name="doLocalAssess">
       <input wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/doLocalAssessRequest" message="tns:doLocalAssess"/>
       <output wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/doLocalAssessResponse" message="tns:doLocalAssessResponse"/>
     </operation>
    ▼<operation name="getDegree">
       <input wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/getDegreeRequest" message="tns:getDegree"/>
       <output wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/getDegreeResponse" message="tns:getDegreeResponse"/>
     </operation>
    ▼<operation name="finish">
       <input wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/finishRequest" message="tns:finish"/>
       <output wsam:Action="http://CSP_WSRA_Proxy/csp_wsra_proxy_base/finishResponse" message="tns:finishResponse"/>
     </operation>
    </portType>
  ▶<binding name="csp_wsra_proxy_basePortBinding" type="tns:csp_wsra_proxy_base">...</binding>
  ▶<service name="csp_wsra_proxy_baseService">...</service>
  </definitions>
```

Fonte: Própria.

Durante a execução da análise de risco o RACloud-Prototype realiza invocações ao método WSRAProxy da classe CSPAgent, solicitando que seja executado o WSRA Proxy de determinada ameaça ou vulnerabilidade. O método WSRAProxy faz então uso da interface CspWsraProxyBase para invocar o respectivo WSRA Proxy do projeto RACloud-CSP-WSRA-Proxy.

4.6 PROJETO RACLOUD-CSP-WSRA-PROXY

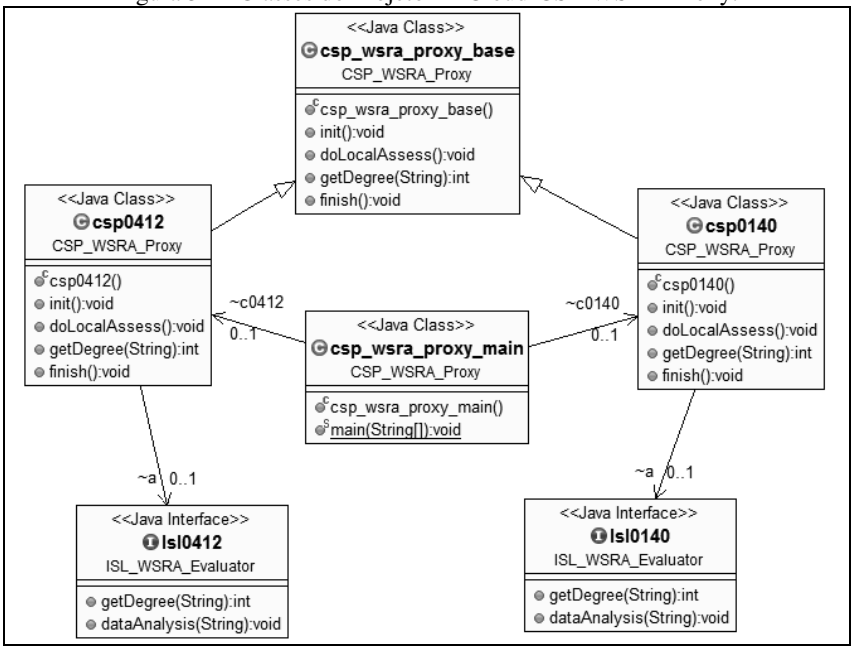
O projeto RACloud-CSP-WSRA-Proxy deve ser desenvolvido pela própria entidade CSP com o objetivo de implementar a coleta de informações locais (no ambiente do CSP) e a invocação dos WSRAs de avaliação das entidades ISL.

O CSP deve especificar e desenvolver WSRAs Proxy para cada ameaça ou vulnerabilidade na qual deseja ter seu ambiente de computação em nuvem analisado. O desenvolvimento dos WSRAs Proxy do CSP deve seguir a especificação WSRA Proxy do modelo

RACloud, conforme definido na Figura 31. Este requisito possibilita que o CSP-Agent possa invocar os WSRAs Proxy sem ter que fazer a importação de todas as interfaces Proxy especificadas pela entidade CSP.

A Figura 32 apresenta as classes e interfaces integrantes de um modelo de especificação do projeto RACloud-CSP-WSRA-Proxy. Neste modelo são propostos dois WSRAs Proxy específicos, chamados de csp0412 e csp0140. Estas duas classes herdam da classe csp_wsra_proxy_base, a qual foi especificada a partir da interface CspWsraProxyBase do projeto RACloud-CSP-Agent, a qual segue a especificação de WSRA Proxy do modelo RACloud definição na seção 3.3.2.

Figura 32 – Classes do Projeto RACloud-CSP-WSRA-Proxy.



Fonte: Própria.

As classes csp0412 e csp0140 são instanciadas pela classe principal do projeto (csp_wsra_proxy_main) e aguardam por solicitações vindas do projeto RACloud-CSP-Agent, via interface padrão para invocação de WSRAs Proxy. Ao serem solicitadas, estas classes realizam a coleta de dados locais do ambiente do CSP e

repassam estas informações para suas respectivas interfaces WSRA de avaliação do projeto RACloud-ISL-WSRA-Evaluator.

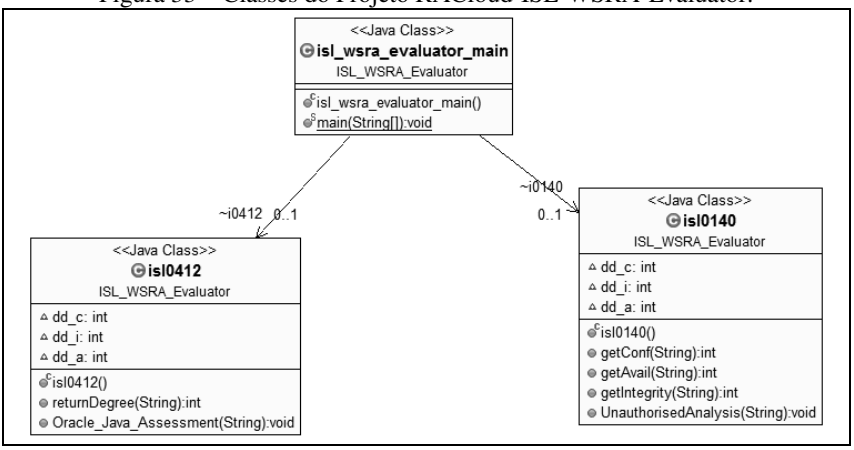
4.7 PROJETO RACLOUD-ISL-WSRA-EVALUATOR

Da mesma forma como ocorre com o projeto RACloud-CSP-WSRA-Proxy, o projeto RACloud-ISL-WSRA-Evaluator também não é desenvolvido pela entidade que provê o RACloud, mas sim por uma ou várias entidades ISL que proveem WSRAs de análise de ameaças ou vulnerabilidades.

Diferentemente do que ocorre no projeto RACloud-CSP-WSRA-Proxy com os WSRAs Proxy, os WSRAs de avaliação do ISL não seguem a um padrão específico de interface, pois estes necessitam de ampla flexibilidade para implementação de suas avaliações. Isto faz com que, na fase de especificação de risco, o CSP precise importar as interfaces de WSRA do ISL para poder desenvolver seus WSRAs Proxy.

A Figura 33 apresenta as classes integrantes de um modelo de especificação do projeto RACloud-ISL-WSRA-Evaluator.

Figura 33 – Classes do Projeto RACloud-ISL-WSRA-Evaluator.



Fonte: Própria.

Seguindo o mesmo modelo apresentado na Figura 32, neste modelo são propostos dois WSRAs de avaliação, representados pelas classes isl0412 e isl0140. Estes WSRAs de avaliação de ameaças ou vulnerabilidades são invocados pelo projeto RACloud-CSP-WSRA-

Proxy via interfaces isl0412 e isl0140 (Figura 32) e realizam a quantificação dos graus de confidencialidade, integridade e disponibilidade, com base nas informações coletadas e enviadas a eles pelo WSRA Proxy.

5 EXPERIMENTOS SIMULADOS COM O PROTÓTIPO

Este capítulo descreve os experimentos simulados realizados a partir do protótipo RACloud previamente descrito. Os experimentos foram realizados em ambiente e com valores controlados, com o objetivo de melhor demonstrar as características de funcionamento do protótipo, e consequentemente do modelo RACloud (SILVA, 2015).

A primeira seção deste capítulo descreve a configuração e execução do ambiente da entidade RAP, que consiste na disponibilização do modelo RACloud a outras entidades do modelo.

A segunda e terceira seções correspondem a fase de especificação do risco do modelo RACloud. A segunda seção descreve a especificação dos RDLs necessários à realização dos experimentos simulados, enquanto que a terceira seção apresenta a configuração e execução dos ambientes dos agentes CC, CSP e ISL.

As seções quatro e cinco correspondem a fase de análise do risco do modelo RACloud. A seção quatro descreve a quantificação dos elementos básicos de risco, enquanto a seção cinco detalha a correlação de eventos e riscos e a geração do RDL de risco resultante para a entidade CC.

5.1 AMBIENTE DA ENTIDADE RAP

Para o estabelecimento do ambiente de experimentos inicialmente foram implementados os projetos que são de responsabilidade da entidade RAP, ou seja, do provedor do modelo RACloud. Neste sentido foram implementadas as camadas Core Layer e Conn Layer (projeto RACloud-Prototype) e os agentes CC, CSP e ISL (projetos RACloud-CC-Agent, RACloud-CSP-Agent e RACloud-ISL-Agent, respectivamente), conforme Figura 19 da seção 3.4.1.

As interfaces web services da camada Conn Layer (ConnCSP, ConnCC e ConnISL) foram geradas a partir do projeto RACloud-Prototype e importadas respectivamente em cada agente, conforme detalhado nos anexos A.1 e A.2.

Da mesma forma, as interfaces para que o Core Layer possa se comunicar com os agentes foram geradas a partir de cada agente e importadas no projeto RACloud-Prototype, conforme anexos A.3 e A.4.

O agente CSP necessita ainda de comunicação com os WSRAs Proxy da entidade CSP, então este precisa ter acesso a interface CspWsraProxyBase (Figura 30) para tal comunicação. O apêndice A.5

detalha a geração da interface web service do WSRA Proxy (CspWsraProxyBase) a partir de um modelo de projeto RACloud-CSP-WSRA-Proxy, enquanto o apêndice A.6 detalha importação desta interface no projeto RACloud-CSP-Agent.

Com isto, a parte do modelo RACloud que compete ao RAP está pronta para ser disponibilizada às entidades CC, CSP e ISL, e o projeto RACloud-Prototype pode ser executado. O apêndice B.1 descreve a execução do projeto RACloud-Prototype pela entidade RAP.

5.2 ESPECIFICAÇÃO DOS RDLs

A fase de especificação do risco nos experimentos simulados com o protótipo inicia-se com a especificação dos RDLs necessários para a execução da análise de risco.

Foram especificados quatro ativos de informação para o agente CC. O Quadro 14 apresenta um resumo dos ativos de informação especificados, enquanto o apêndice D.1 apresenta o RDL de ativos de informação completo.

No apêndice D.1 pode-se observar que no RDL de ativos de informação já estão especificados os graus de impacto para confidencialidade, integridade e disponibilidade desejados pela entidade CC para cada ativo de informação, bem como a categoria de cada ativo de informação especificado. Para este experimento simulado os valores de confidencialidade, integridade e disponibilidade para os ativos de informação foram selecionados de modo aleatório, com o único objetivo de experimentação do modelo proposto.

Quadro 14 – Ativos de informação especificados para experimento.

Id A	Descrição	Asset Category	DIc(%)	DIi(%)	DIa(%)
001	Contratos de clientes	File	75	80	68
002	Informações financeiras	Database	80	90	60
003	Sistema de Pedidos	CC-Software	60	85	80
004	Sistema help desk	CSP-Software	40	70	85

Para o agente ISL foram especificados sete itens de vulnerabilidade, conforme Quadro 15. Os itens de vulnerabilidade foram selecionados a partir de vulnerabilidades publicadas na base CVE. Foram selecionados diferentes itens de vulnerabilidade de modo a se obter uma abrangência sobre diferentes categorias de recursos tratadas pelo modelo RACloud.

Quadro 15 – Vulnerabilidades especificadas para experimento.

Id V	Descrição	Resource Category	Referência
9593	Apache CloudStack before 4.3.2 allow obtain private key	Communication System	CVE-2014-9593
0140	Red Hat CloudForms 3.1 allow Unauthorised actions	Cloud System	CVE-2014-0140
1609	MongoDB before 2.4.13 allows denial of service	Database	CVE-2015-1609
3367	Cross-site scripting (XSS) vulnerability in the vCloud VMWare	VM System	CVE-2014-3367
0640	HSL feature in Cisco IOS XE 2.x Dos via IP	Communication System	CVE-2015-0640
0412	Oracle Java SE 6u85 vulnerability related to JAX-WS	Framework	CVE-2015-0412
2576	MySQL 1.5.1 and earlier integrity failure	Database	CVE-2015-2576

O apêndice D.2 detalha o RDL de definição de vulnerabilidades utilizado pelo agente ISL nos experimentos simulados com o protótipo. Para cada item de vulnerabilidade o RDL especifica as propriedades de

segurança da informação as quais o item se relaciona. Esta informação é essencial para a posterior realização da correlação entre vulnerabilidades e ameaças. O Quadro 16 apresenta um resumo das propriedades de segurança da informação aplicáveis a cada item de vulnerabilidade, com base no RDL definido para o agente ISL do protótipo (apêndice D.2).

Quadro 16 – Propriedades de segurança por vulnerabilidades especificadas.

Id V	c	i	a
9593	X	X	
0140	X	X	X
1609			X
3367	X	X	X
0640			X
0412	X	X	X
2576		X	

Da mesma forma como foi realizado com as vulnerabilidades, foram especificados seis itens de ameaças (Quadro 17). As ameaças selecionadas para o experimento simulado com o protótipo foram extraídas de recomendações da ISO 25005 (ISO 27005, 2011) e CSA Guide (CLOUD SECURITY ALLIANCE, 2011). Para fins de experimento do protótipo, foram selecionadas ameaças compatíveis com as vulnerabilidades previamente especificadas.

Quadro 17 – Ameaças especificadas para experimento.

Id T	Descrição	Resource Category	Referência
459	Remote spying	Communication System	ISO 27005
423	Saturation of the system	Cloud System	ISO 27005
445	Corruption of data	Database	ISO 27005
254	Inter-VM violation	VM System	CSA Guide
656	Tampering on transit	Communication System	CSA Guide
443	Spoofing of user	Framework	CSA Guide

O apêndice D.3 detalha o RDL de definição de ameaças utilizado pelo agente ISL nos experimentos simulados com o protótipo. Da

mesma forma como ocorre com as vulnerabilidade, o RDL de ameaças define as propriedades de segurança da informação exploradas por cada item de ameaça. O Quadro 18 apresenta um resumo das propriedades de segurança da informação aplicáveis a cada item de ameaça, com base no RDL definido para o agente ISL do protótipo (apêndice D.3).

Quadro 18 – Propriedades de segurança por ameaças especificadas.

Id T	c	i	a
459	X		
423			X
445		X	
254	X	X	X
656	X	X	
443	X	X	X

Os RDLs de ativos de informação, ameaças e vulnerabilidades acima apresentados foram especificados com objetivo de experimento simulado com o protótipo do modelo RACloud, em um ambiente real estas informações seriam especificadas por uma entidade CC (no caso de ativos de informação) e uma ou várias entidades ISL (no caso de vulnerabilidades e ameaças).

5.3 AMBIENTE DAS ENTIDADES CC, CSP E ISL

Uma vez especificados os RDLs, ainda na fase de especificação do risco, a entidade ISL deve especificar e implementar o projeto RACloud-ISL-WSRA-Evaluator, onde se definirá os WSRAs de avaliação de cada item de vulnerabilidade ou ameaça previamente especificado nos RDLs da entidade ISL.

Foram especificados e implementados no projeto RACloud-ISL-WSRA-Evaluator sete classes para os itens de vulnerabilidade especificados no RDL de vulnerabilidades e seis classes para os itens de ameaças especificados no RDL de ameaças. Cada uma destas classes corresponde a um WSRAs de avaliação da entidade ISL. O apêndice A.7 detalha a geração dos web services destes WSRAs.

A entidade CSP que deseja ter seu ambiente de computação em nuvem analisado deve implementar o projeto RACloud-CSP-WSRA-Proxy com os WSRAs Proxy das avaliações desejadas. Para fins de experimento simulado com o protótipo foram especificados e implementados no projeto RACloud-CSP-WSRA-Proxy os WSRAs

Proxy de todas as vulnerabilidades e ameaças especificadas no projeto RACloud-ISL-WSRA-Evaluator. Para tanto, o projeto RACloud-CSP-WSRA-Proxy precisa importar as interfaces de análise de ameaças e vulnerabilidades do projeto RACloud-ISL-WSRA-Evaluator. O apêndice A.8 detalha a importação das interfaces de análise de ameaças e vulnerabilidades no projeto RACloud-CSP-WSRA-Proxy.

Uma vez realizada a configuração de comunicação entre os web services dos diferentes projetos, há a necessidade de se definir arquivos de configuração para os diferentes agentes participantes do modelo RACloud.

O apêndice C.1 detalha o arquivo de configuração do agente CC, onde estão definidos o nome do CC e do CSP, além da porta em que as interfaces do CC atendem às requisições do projeto RACloud-Prototype. O arquivo de configuração do agente CC também define o local da base de RDLs do CC e o local para armazenamento dos RDLs de resultado da análise de risco.

O apêndice C.2 detalha o arquivo de configuração do agente CSP. Este arquivo especifica informações básicas como o nome do CSP no RACloud e a porta em que as interfaces do CSP atendem suas requisições, porém também são definidas neste arquivo informações mais específicas do CSP, como a identificação dos RDLs de vulnerabilidades e ameaças nos quais o CSP deseja se inscrever, e a definição de qual WSRA Proxy publicado pelo CSP corresponde a qual WSRA de avaliação do ISL.

O apêndice C.3 detalha o arquivo de configuração do agente ISL. Neste arquivo são definidos apenas o nome e porta do ISL, além da localização da base de RDLs de vulnerabilidades e ameaças do ISL.

Uma vez especificados os RDLs e arquivos de configuração dos agentes ISL, CSP e CC, estes podem ser executados por suas respectivas entidades responsáveis. O apêndice B.2 detalha a execução por parte da entidade ISL, a qual deve executar em seu ambiente os projetos RACloud-ISL-Agent e RACloud-ISL-WSRA-Evaluator. O apêndice B.3 detalha a execução por parte da entidade CSP, cuja responsabilidade abrange os projetos RACloud-CSP-Agent e RACloud-CSP-WSRA-Proxy. Finalmente, o apêndice B.4 detalha a execução sob responsabilidade da entidade CC, ou seja, a execução do projeto RACloud-CC-Agent.

Com a execução de todos os agentes, estes se registram na Core Layer via Conn Layer e publicam seus RDLs de ameaças e vulnerabilidades (no caso do agente ISL). Isto conclui a fase de especificação do risco conforme apresentado na seção 3.4.2. O apêndice

F.1 apresenta o log de execução do RACloud-Prototype e dos agentes CC, CSP e ISL na fase de especificação do risco.

5.4 QUANTIFICAÇÃO DOS ELEMENTOS BÁSICOS DE RISCO

A fase de análise do risco inicia-se com a entidade CC invocando o comando "doRiskAnalysis" no console do projeto RACloud-CC-Agent. Então ocorre a quantificação de deficiências das vulnerabilidades e de exposição das ameaças, conforme descrito na seção 3.4.3.

Nos RDLs de vulnerabilidades e ameaças foram especificados sete itens de vulnerabilidades (Quadro 15) e seis itens de ameaças (Quadro 17). Durante a fase de análise do risco na execução dos experimentos simulados com o protótipo foram invocados os WSRAs Proxy da entidade CSP e os WSRAs de avaliação da entidade ISL, os quais quantificam o grau de deficiência para cada um dos itens de vulnerabilidade e o grau de exposição para cada um dos itens de ameaça, para cada uma das propriedades de segurança da informação, quando aplicáveis ao item.

Quadro 19 – Resultado da análise das vulnerabilidades.

Id V	DDc(%)	DDi(%)	DDa(%)
9593	70	50	30
0140	90	80	70
1609	–	–	45
3367	70	50	30
0640	–	–	78
0412	40	30	90
2576	–	55	–

O Quadro 19 apresenta os resultados da quantificação dos sete itens de vulnerabilidade previamente especificados, enquanto o Quadro 20 apresenta os resultados da quantificação dos seis itens de ameaça. Destaca-se que os valores apresentados nestes quadros (quadro 19 e quadro 20) são resultantes das implementações simuladas dos WSRAs de vulnerabilidades e ameaças.

Os anexos F.3, F.4 e F.5 apresentam os logs de execução dos projetos RACloud-CSP-Agent, RACloud-CSP-WSRA-Proxy e RACloud-ISL-WSRA-Evaluator durante a quantificação de vulnerabilidades e ameaças.

Destaca-se que os resultados de quantificação de vulnerabilidades e ameaças retornados pelos WSRAs de avaliação são valores previamente definidos, com o objetivo demonstrar as funcionalidades do modelo RACloud. Os valores foram definidos nas implementações simuladas dos WSRAs, de modo aleatório, com o único objetivo de demonstrar as funcionalidades do modelo proposto.

Quadro 20 – Resultado da análise das ameaças.

Id T	DEc(%)	DEi(%)	DEa(%)
459	70	–	–
423	–	–	80
445	–	90	–
254	90	40	30
656	70	60	–
443	90	90	60

Também no início da fase de análise do risco dos experimentos simulados com o protótipo o projeto RACloud-Prototype realiza uma consulta ao CC Agent quanto aos itens de ativos de informação e seus respectivos valores de impacto (Quadro 14). O apêndice F.2 apresenta a execução do projeto RACloud-Prototype durante a execução dos experimentos simulados, onde através da legenda ADD-ASSET é possível identificar os ativos de informação obtidos do CC Agent.

5.5 CORRELAÇÃO DE EVENTOS E RISCOS

Uma vez quantificados os elementos básicos do risco (vulnerabilidades, ameaças e ativos de informação), a execução dos experimentos simulados com o protótipo passa para a correlação entre vulnerabilidades e ameaças para a formação de eventos de incidentes de segurança da informação.

Conforme descrito na seção 3.2.3, ameaças e vulnerabilidades se correlacionam no modelo RACloud para a formação de eventos de incidentes de segurança da informação quando atuam sobre o mesmo RC e possuem propriedades de segurança compatíveis.

O Quadro 21 demonstra o resultado da execução da função de correlação de eventos com os RDLs de vulnerabilidades (apêndice D.2) e ameaças (apêndice D.3) previamente apresentados.

As linhas do Quadro 21 contém o cruzamento das ameaças e vulnerabilidades que atuam sobre a mesma categoria de recurso. As

colunas “c”, “i” e “a” representam as propriedades de segurança da informação e as letras V e T nestas colunas apresentam as propriedades que são aplicáveis a vulnerabilidades e ameaças, respectivamente. A última coluna contém as propriedades que são comuns a vulnerabilidade e ameaça em questão.

Quadro 21 – Correlação de eventos entre ameaças e vulnerabilidades.

Id V	Id T	Resource Category	c	i	a	Relação
9593	459	Communication System	VT	V		c
9593	656	Communication System	VT	VT		c,i
0140	423	Cloud System	V	V	VT	a
1609	445	Database		T	V	
3367	254	VM System	VT	VT	VT	c,i,a
0640	459	Communication System	T		V	
0640	656	Communication System	T	T	V	
0412	443	Framework	VT	VT	VT	c,i,a
2576	445	Database		VT		i

O cruzamento das vulnerabilidades e ameaças que atuam sobre a mesma categoria de recurso gerou nove itens de eventos no Quadro 21, porém a identificação de propriedades de segurança compatíveis entre os itens reduziu os eventos correlacionados para somente seis eventos válidos. Sendo que somente dois são válidos para as três propriedades de segurança da informação, um é válido para duas propriedades e três são válidos somente para uma das propriedades.

Os seis itens de eventos resultantes da função de correlação de eventos são passados para a função de cálculo da probabilidade do evento, que correlaciona as variáveis DD das vulnerabilidades com as variáveis DE das ameaças, porém apenas para as propriedades de segurança da informação que sejam válidas para cada evento.

Quadro 22 – Resultado do cálculo da probabilidade dos eventos.

Id E	Pc(%)	Pi(%)	Pa(%)
9593@459	70	–	–
9593@656	70	55	–
0140@423	–	–	75
3367@254	80	45	30
0412@443	65	60	75
2576@445	–	72	–

O Quadro 22 apresenta o resultado da função de cálculo da probabilidade de eventos, onde é possível observar que somente fazem parte deste conjunto os itens de eventos que foram correlacionados pela função de correlação de eventos e somente foram atribuídos valores de probabilidade as propriedades de segurança da informação aplicáveis a cada item de evento, conforme resultado da função de correlação de eventos. Neste experimento simulado, para fins de validação do protótipo, a função de probabilidade realiza uma média aritmética simples sobre as variáveis de grau de exposição e grau de deficiência. O apêndice F.2 (legenda PROB-FUNC) apresenta o log de execução do projeto RACloud-Prototype em relação à correlação de eventos e cálculo da probabilidade.

Após a correlação de eventos e cálculo da probabilidade, o experimento simulado no protótipo prossegue com a correlação de riscos (eventos e ativos de informação) e o cálculo final dos itens de risco.

O Quadro 23 apresenta a correlação realizada pelo RACloud-Prototype entre os eventos de incidentes de segurança da informação (Quadro 22) e os ativos de informação especificados no RDL de ativos de informação da entidade CC (Quadro 14).

A correlação resultante no Quadro 23 segue a modelagem do risco do modelo RACloud conforme seção 3.2.3 (Quadro 13). É possível observar que o ativo de informação Id=001 (Contratos de clientes) com AC=File foi correlacionado com os eventos de RCs com RL=1 (itens Id R 1 a 4). O ativo de informação 002 (Informações financeiras) com AC=Database foi correlacionado com o evento de RC Database, além de todos os eventos de RCs com RLs=1 (itens Id R 5 a 9). O ativo de informação 003 (Sistema de pedidos) de AC=CC-Software foi correlacionado com todos os itens de evento cuja RC seja de RL=1 e também com a RC Database e RC Framework, visto que o item de RDL deste ativo de informação (apêndice D.1) sinaliza que ele faz uso destes recursos (database e framework) do CSP (itens Id R 10 a 15). O ativo de

informação 004 (Sistema help desk) correlaciona também com todos os eventos de RCs com RL=1 e com a RC Framework, visto que o item de RDL deste ativo de informação (apêndice D.1) não prevê o uso do recurso database (itens Id R 16 a 20).

Quadro 23 – Correlação entre Eventos e Ativos de Informação.

Id E	Id A	Id R	Resource Category	Asset Category
9593@459	001	1	Communication System	File
9593@656	001	2	Communication System	
0140@423	001	3	Cloud System	
3367@254	001	4	VM System	
9593@459	002	5	Communication System	Database
9593@656	002	6	Communication System	
0140@423	002	7	Cloud System	
3367@254	002	8	VM System	
2576@445	002	9	Database	
9593@459	003	10	Communication System	CC-Software
9593@656	003	11	Communication System	
0140@423	003	12	Cloud System	
3367@254	003	13	VM System	
0412@443	003	14	Framework	
2576@445	003	15	Database	
9593@459	004	16	Communication System	CSP-Software
9593@656	004	17	Communication System	
0140@423	004	18	Cloud System	
3367@254	004	19	VM System	

0412@443	004	20	Framework	

Finalmente, o Quadro 24 apresenta o resultado da função de cálculo de risco implementada no projeto RACloud-Prototype. Esta função teve como entrada os vinte itens de risco correlacionados pela função de correlação de risco (Quadro 23) e como saída os graus de risco para as propriedades de confidencialidade, integridade e disponibilidade, quando aplicáveis a cada evento de incidente de segurança da informação. Neste experimento simulado, para fins de validação do protótipo, a função de risco realiza uma média aritmética simples sobre as variáveis de probabilidade e grau de impacto. O apêndice F.2 (legenda RISK-FUNC) apresenta o log de execução no projeto RACloud-Prototype em relação à função de cálculo do risco.

Quadro 24 – Resultado do cálculo do risco.

Id R	DRc(%)	DRi(%)	DRa(%)
1	72	–	–
2	72	67	–
3	–	–	71
4	77	62	49
5	75	–	–
6	75	72	–
7	–	–	67
8	80	67	45
9	–	81	–
10	65	0	–
11	65	70	–
12	–	–	77
13	70	65	55
14	62	72	77
15	–	78	–
16	55	–	–
17	55	62	–
18	–	–	80
19	60	57	57
20	52	65	80

Feito o cálculo do risco, a última tarefa do RACloud-Prototype é gerar o RDL de risco resultante e retorná-lo para a entidade CC através do RACloud-CC-Agent. O apêndice F.6 apresenta o log de execução do projeto RACloud-CC-Agent por onde a entidade CC recebe o RDL de risco resultante, enquanto o apêndice E apresenta o conteúdo completo

do RDL de risco resultante gerado pelo experimento simulado do protótipo RACloud e recebido pela entidade CC.

6 RESULTADOS E DISCUSSÃO

Este capítulo descreve os resultados e discussão deste trabalho de tese obtidos com a especificação, desenvolvimento e experimentos simulados do modelo RACloud.

6.1 RESULTADOS

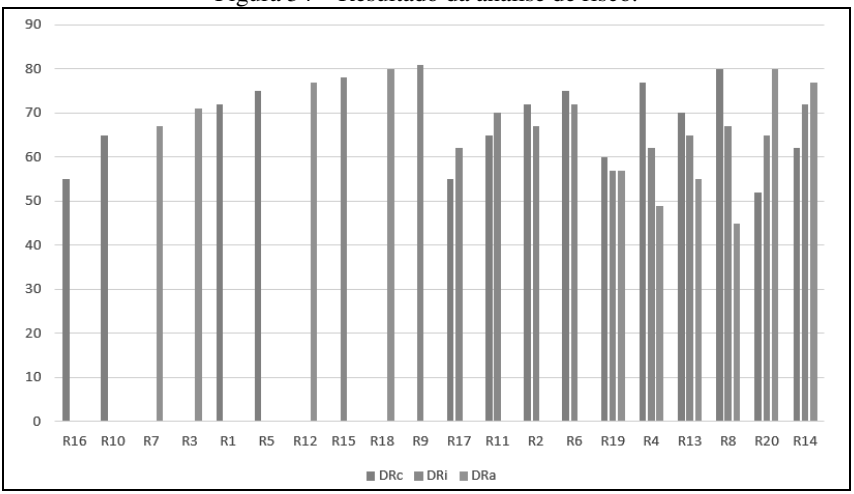
Para fins de experimentos do modelo RACloud e discussão, foi desenvolvido um protótipo do modelo, conforme apresentado no Capítulo 5. A partir do protótipo desenvolvido foram executadas as fases de especificação de risco e avaliação de risco em um ambiente controlado para experimentos.

Na fase de especificação de risco, foram especificados 7 registros RDL de vulnerabilidades (Quadro 15), 6 registros RDL de ameaças (Quadro 17) e 4 registros RDL de ativos de informação (Quadro 14). Os registros RDL de ameaças e vulnerabilidades foram especificados conforme ameaças e vulnerabilidades disponíveis em CVE – Common Vulnerabilities and Exposures. Também foram desenvolvidos os WSRAs e WSRAs Proxy para os 13 registros de ameaças e vulnerabilidades especificados.

Na fase de avaliação de risco foram executados os WSRAs Proxy e WSRAs, gerando os valores de grau de deficiência e grau de exposição para cada registro de vulnerabilidade (Quadro 19) e ameaça (Quadro 20), respectivamente. Os registros de vulnerabilidades e ameaças foram correlacionados pelo componente Analysis Manager (Quadro 21) gerando 6 eventos de correlação válidos a partir de 9 eventos possíveis (Quadro 21). Os registros de eventos válidos foram correlacionados com os registros de ativos de informação (Quadro 23), gerando 20 cenários de risco (Quadro 24).

A Figura 34 apresenta o resultado do cálculo das variáveis DRc, DRi e DRa para os 20 cenários de risco (R1 a R20) especificados no protótipo e nos experimentos simulados.

Figura 34 – Resultado da análise de risco.



Fonte: Própria.

O gráfico da Figura 34 apresenta, por exempo, que o cenário de risco R16 possui um risco de confidencialidade de 55%. Este cenário especifica como ativo de informação o Sistema Helpdesk, com vulnerabilidade o registro CVE 9593 e ameaça a espionagem remota.

A Figura 35 apresenta o resultado da avaliação de risco gerado pelo protótipo do modelo RACloud para os cenários de risco R16 e R14. Para cada cenário de risco é possível observar o resultado das variáveis de probabilidade e risco. Também é possível observar uma breve descrição dos itens de ameaças, vulnerabilidades e ativos de informação e o valor de suas respectivas variáveis de grau de exposição, grau de deficiência e grau de impacto, para cada uma das propriedades de segurança, respectivamente.

Figura 35 – RDL de risco resultante.

```
▼<risk_item DRa="0" DRc="55" DRi="0" id="16">
   <informationAsset DIa="85" DIc="40" DIi="70" id="004">Sistema help desk</informationAsset>
  ▼<event Pa="0" Pc="70" Pi="0" id="9593@459">
    ▼<vulnerability DDa="30" DDc="70" DDi="50" id="9593">
       Apache CloudStack before 4.3.2 allow obtain private key
     </vulnerability>
     <threat DEa="0" DEc="70" DEi="0" id="459">Remote spying</threat>
   </event>
 </risk_item>

▼<risk_item DRa="77" DRc="62" DRi="72" id="14">
   <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de Pedidos</informationAsset>
  ▼<event Pa="75" Pc="65" Pi="60" id="0412@443">
    ▼<vulnerability DDa="90" DDc="40" DDi="30" id="0412">
       Oracle Java SE 6u85 vulnerability related to JAX-WS
     </vulnerability>
     <threat DEa="60" DEc="90" DEi="90" id="443">Spoofing of user</threat>
   </event>
 </risk item>
```

Fonte: Própria.

Com as informações resultantes da análise de risco o CC pode decidir alocar ou não seus ativos de informações em um determinado CSP, ou então remover seus sistemas de um CSP que apresente grandes riscos.

6.2 DISCUSSÃO

O modelo proposto visa reduzir as três principais deficiências apresentadas pelos modelos atuais de análise de risco em nuvem (seção 2.5): deficiência na abrangência dos requisitos, deficiência na aderência ao cliente e deficiência na independência dos resultados.

A redução da deficiência de aderência ocorre quando o modelo proposto inclui o CC como uma entidade fundamental no processo de análise de risco. No modelo RACloud a entidade CC age de modo ativo na análise de risco, definindo ativos de informação e quantificando impactos sobre estes ativos.

O CC é a entidade mais apta para a definição de impactos, pois é a entidade que melhor conhece a relevância de cada ativo de informação dentro de sua área de atuação. Sendo assim, é responsabilidade do CC informar qual será o impacto se determinado sistema, base de dados ou arquivo tiver sua integridade, confidencialidade ou disponibilidade prejudicada. As entidades CSP e ISL não possuem competência para identificar ou quantificar impactos sobre ativos de informação, pois não são especialistas na área de negócio do CC.

O modelo RACloud atua na redução da deficiência de abrangência na medida em que introduz a entidade ISL. Sendo o ISL uma entidade especializada em segurança da informação, é a entidade

mais indicada para definir requisitos de segurança, ameaças e vulnerabilidades (especificação dos RDLs), bem como definir como as ameaças e vulnerabilidades devem ser analisadas (especificação dos WSRAs).

A redução da deficiência na independência dos resultados ocorre pelo fato de que no modelo RACloud o CSP possui responsabilidades mais restritas do que nos modelos tradicionalmente apresentados pelos trabalhos correlatos.

Tradicionalmente o CSP é responsável pela definição dos requisitos de segurança e pelos testes que são aplicados para avaliação do risco de seu próprio ambiente. Neste cenário, no qual o CSP possui mais responsabilidades na análise de risco, existe mais possibilidades de que a análise de risco seja tendenciosa aos interesses do CSP, visto que ele próprio é responsável por todo o processo de análise de risco. A inclusão da entidade ISL retira responsabilidades tradicionalmente atribuídas ao CSP, como a identificação e análise de ameaças e vulnerabilidades.

O modelo proposto permite que vários ISLs atuem na definição de RDLs e WSRAs de forma conjunta. Desta forma as definições de risco podem vir de diferentes origens e podem ser constantemente atualizadas de modo dinâmico e colaborativo, formando uma base definições de risco em nuvem ampla e independente.

A forma como os WSRAs são especificados também é uma característica que impacta na melhoria da abrangência. A utilização de Web Services para especificar os requisitos de segurança permite que estes sejam independentes de plataforma e possam ser requisitados por qualquer CSP. Também permite o uso de uma ampla variedade de técnicas para a quantificação das ameaças e vulnerabilidades, pois o limite será apenas definido pela linguagem de programação escolhida para implementação do WSRA.

Os trabalhos correlatos de análise de risco em nuvem não consideram o papel da entidade CC na análise de risco. Estes trabalhos geralmente focam na avaliação de vulnerabilidades pelo próprio CSP, sem considerar o impacto que a vulnerabilidade irá causar sobre os diferentes ativos de informação do CC. Ao atribuir a responsabilidade pela identificação e quantificação do impacto ao CC este trabalho visa compartilhar as variáveis do risco entre diferentes entidades, desta forma a responsabilidade pela quantificação das variáveis da análise de risco não fica centralizada em apenas uma entidade específica.

Conforme os modelos apresentados por Chen (2012), Ullah (2012) e Hale (2012) na seção de trabalhos correlatos, figuras 9, 10 e 11

respectivamente, pode-se observar a inexistência de componentes correspondentes ao ISL proposto por este presente trabalho de tese. Também pode-se observar a inexistência de participação ativa do CC durante a execução das análises nestes modelos.

O CSP é a entidade que será analisada, logo esta não tem competência para definir quaisquer dos valores da análise de risco, pois isto poderia tornar a análise de risco menos independente. O papel do CSP é apenas informar os dados solicitados pelo ISL, a fim de que o próprio ISL faça a quantificação dos requisitos de segurança e a geração dos resultados da análise de risco.

Considerando o papel desempenhado pelo CSP no modelo proposto, este possui atribuições mais bem definidas e restritas em comparação aos modelos identificados nos trabalhos correlatos. Porém o CSP ainda tem a atribuição de fornecer os dados para a execução das quantificações das variáveis de risco no ISL. Esta característica gera uma limitação no modelo proposto no sentido de que em determinados casos o CSP poderá fornecer dados incorretos ao ISL. Desta forma o resultado da análise de risco terá sua confiabilidade final prejudicada. Cabe ao ISL modelar avaliações de risco que reduzam a possibilidade de fraude nos dados passados pelo ISL e, nos casos em que isto não for possível, a garantia da veracidade das informações passadas pelo CSP ao ISL para execução das análises de risco deve ser gerenciada através de controles não computacionais, como por exemplo, o estabelecimento de contratos de prestação de serviço com cláusulas específicas sobre o fornecimento de informações para a análise de risco.

A definição formal da representação dos riscos através da especificação dos RDLs, bem como a definição de um modelo de correlação entre ameaças e vulnerabilidades para formação de eventos, e entre eventos e ativos de informação para formação de cenários de riscos em nuvem também é uma importante contribuição do modelo RACloud para a análise de risco em nuvem.

Os RDLs permitem que diferentes entidades troquem informações sobre a especificação de ameaças, vulnerabilidades e ativos de informação. É possível que diferentes ISLs desenvolvam seus RDLs para ameaças e vulnerabilidades e que estes sejam integrados através do modelo RACloud para a execução da análise de risco em um CSP específico.

O modelo de correlação de eventos, através da definição de Categorias de Recursos (Quadro 3), permite que diferentes ameaças e vulnerabilidades (inclusive desenvolvidos por diferentes ISLs) sejam correlacionadas em eventos válidos (que fazem sentido) para o cálculo

da probabilidade. Por exemplo, nos experimentos simulados realizados sobre o protótipo do modelo RACloud, o simples cruzamento entre as ameaças e as vulnerabilidades especificadas nos RDLs geraria 42 eventos de incidentes (7 vulnerabilidade X 6 ameaças), muitos destes inválidos ou sem sentido. Porém a aplicação do modelo de correlação de eventos gerou apenas 6 eventos válidos.

Da mesma forma como ocorre com a correlação de eventos, o modelo de correlação de riscos, através da definição de Categorias de Ativos de Informação (Quadro 3), permitem que diferentes eventos possam se correlacionar com diferentes ativos de informação para cenários de incidentes coerentes. Nos experimentos simulados, se fossem desconsiderados os modelos de correlação, os 42 eventos potencialmente gerados resultariam em 168 (42 eventos X 4 ativos de informação) cenários de risco, muitos destes incoerentes. Porém a função de correlação de risco recebeu apenas 6 eventos válidos (Quadro 22) para serem correlacionados com 4 ativos de informação (Quadro 14) resultando em apenas 20 cenários de risco válidos (Quadro 23).

Com o modelo RACloud um CC pode realizar análises em vários CSPs antes de optar pela aquisição de um serviço de computação em nuvem. Também pode realizar análises periódicas de seu provedor atual e compará-las com outros provedores de mercado, optando por mudar ou não de CSP.

7 SÍNTESE DOS RESULTADOS E CONCLUSÃO

Esta tese de doutorado faz a proposição de um modelo computacional no qual o cliente possa realizar uma análise de risco de segurança da informação em um ambiente de nuvem.

O modelo proposto está intimamente associado ao ambiente de nuvem devido a sua arquitetura especificamente organizada em entidades CC e CSP, sendo estas entidades tradicionalmente identificadas em ambientes de nuvem. A definição de RCs (categorias de recursos) e ACs (categorias de ativos de informação), que permitem a correlação de eventos e riscos, também está intimamente associada ao universo da computação em nuvem, tornando o modelo proposto aderente a tais ambientes.

O modelo proposto demonstra as características de aderência, abrangência e independência dos resultados. É aderente no sentido de que o próprio CC define os níveis de impacto sobre seus ativos de informação. É abrangente no sentido de que uma ou várias entidades ISL podem definir ameaças e vulnerabilidades a serem analisadas. E é independente no sentido de que a responsabilidade do CSP foi consideravelmente reduzida em relação aos modelos tradicionalmente encontrados.

Também no modelo proposto as diferentes entidades envolvidas em uma análise de risco e suas responsabilidades foram definidas. Foi apresentada uma linguagem para especificação de riscos e suas variáveis integrantes. Um modelo de correlação entre os elementos de risco foi descrito. E experimentos simulados para validação do modelo proposto no contexto de ativos de informação foram realizados.

7.1 PRINCIPAIS CONTRIBUIÇÕES

Este trabalho de tese apresentou um modelo para análise de risco no contexto de ativos de informação em ambientes de computação em nuvem – RACloud.

O modelo proposto altera o paradigma geralmente vigente nas pesquisas sobre análise de risco em nuvem, no qual a entidade CSP é responsável pela especificação dos requisitos de segurança e pela execução e análise destes requisitos em seu próprio ambiente, sendo assim a única entidade responsável pelos resultados da análise de risco.

Para reduzir excesso de responsabilidade do CSP na análise de risco, o modelo proposto inclui duas novas entidades com participação ativa na análise de risco, a entidade CC e a entidade ISL.

O modelo apresentado (RACloud) é uma iniciativa no sentido de que o próprio CC possa executar a análise de risco em seu CSP atual ou futuro. E que esta análise de risco seja aderente, abrangente e independente dos interesses do CSP.

As características do modelo proposto apresentadas nesta tese visam gerar uma análise de risco mais confiável para o CC, de modo que este possa escolher seu CSP com base em informações mais consistentes, especificadas e analisadas por uma entidade isenta de interesses, o ISL.

Diversos trabalhos sobre computação em nuvem indicam a falta de confiança do CC em relação ao CSP como sendo um grande motivador para a não aquisição de serviços de computação em nuvem. Uma análise de risco independente pode atuar na redução desta desconfiança e impulsionar a aquisição de serviços de computação em nuvem.

O protótipo desenvolvido e os resultados apresentados demonstram a especificação e execução de uma análise de risco aderente, abrangente e independente, pois a análise não está centralizada no CSP. As identificações e quantificações de ameaças e vulnerabilidades podem ser realizadas por diversos laboratórios de segurança e o impacto sobre os ativos de informação é definido pelo próprio CC.

7.2 TRABALHOS FUTUROS

Vários trabalhos futuros podem ser desenvolvidos a partir do modelo RACloud. Estes trabalhos podem atuar na melhoria ou estudos mais aprofundados das características de aderência, abrangência e independência dos resultados no modelo RACloud.

Quanto à aderência da análise de risco à realidade do CC, é possível o desenvolvimento de um trabalho em relação às ameaças e vulnerabilidades existentes no próprio ambiente do CC. Estas informações poderiam compor a análise de risco do modelo RACloud tornando-o ainda mais aderente ao CC.

Quanto à abrangência, é possível o desenvolvimento de estudo mais aprofundados sobre a linguagem de definição de riscos – RDL,

buscando por ameaças ou vulnerabilidades que não seriam contempladas pelo modelo atual.

Quanto à independência dos resultados, podem ser desenvolvidas pesquisas para avaliação do nível de confiança dos dados informados pelo CSP ao ISL durante a análise de risco.

Existe ainda a necessidade de extensão deste trabalho a fim de que o modelo também possa sugerir os controles ou contra medidas para que os CSPs possam mitigar seus riscos.

A análise dos dados resultantes da análise de risco bem como o desenvolvimento de análises com foco mais específico em recursos computacionais também pode ser uma extensão para trabalhos futuros, além da inclusão de conceitos de SLA na análise de risco.

Outro proposta de trabalho futuro consiste em integrar o modelo proposto com ferramentas de verificação de vulnerabilidades (ex. nmap, nessus ou openVAS). Desta forma, os WSRAs seriam realizados através das ferramentas de verificação de vulnerabilidades.

REFERÊNCIAS

ALEBRAHIM, A.; HATEBUR, D.; GOEKE, L., "Pattern-based and ISO 27001 compliant risk analysis for cloud systems," Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop on , vol., no., pp.42,47, 25-25 Aug. 2014.

ALFATH, A. ; BAINA, K. ; BAINA, S, “Cloud computing security: Fine-grained analysis and security approaches”, Security Days (JNS3), 2013 National Digital Object Identifier: 10.1109/JNS3.2013.6595465, Publication Year: 2013, Page(s): 1- 6;

BHENSOOK, N. ; SENIVONGSE, T., “An assessment of security requirements compliance of cloud providers”. Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on. Digital Object Identifier: 10.1109/CloudCom.2012.6427484. Publication Year: 2012 , Page(s): 520- 525.

BLEIKERTZ, S.; MASTELIC, T.; PAPE, S.; PIETERS, W.; DIMKOV, T., “Defining the Cloud Battlefield - Supporting Security Assessments by Cloud Customers”, Cloud Engineering (IC2E), 2013 IEEE International Conference on, Digital Object Identifier: 10.1109/IC2E.2013.31, Publication Year: 2013, Page(s): 78- 87.

CAYIRCI, E.; GARAGA, A.; Santana de Oliveira, A.; ROUDIER, Y., "A Cloud Adoption Risk Assessment Model", Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on , vol., no., pp.908,913, 8-11 Dec. 2014

CHEN, J.; Y, WANG and X. WANG, "On-Demand Security Architecture for Cloud Computing," Computer, IEEE, vol.45, no.7, pp.73,78, July 2012 doi: 10.1109/MC.2012.120.

CLOUD SECURITY ALLIANCE, “Security Guidance for Critical Areas of Focus in Cloud Computing”. https://cloudsecurityalliance.org/guidance/ csaguide.v3.0.pdf, 2011.

CLOUD SECURITY ALLIANCE, “The Notorious Nine: Cloud Computing Top Threats”. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/ The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf, 2013.

DEY, Sujit., “Mobile cloud applications: opportunities, challenges and directions”. Proceeding MobileCloud '13. Proceedings of the first international workshop on Mobile cloud computing & networking. Pages 1-2.

GUPTA, S.; MUNTES-MULERO, V.; MATTHEWS, P.; DOMINIAK, J.; OMEROVIC, A.; ARANDA, J.; SEYCEK, S., "Risk-Driven Framework for Decision Support in Cloud Service Selection," Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on , vol., no., pp.545,554, 4-7 May 2015. doi: 10.1109/CCGrid.2015.111

HALE, M. L.; GAMBLE R., "SecAgreement: Advancing Security Risk Calculations in Cloud Services," Services (SERVICES), 2012 IEEE Eighth World Congress on , vol., no., pp.133-140, 24-29 June 2012 doi: 10.1109/SERVICES.2012.31.

HÖFER, C.N. and KARAGIANNIS, G. (2011) “Cloud computing services: taxonomy and comparison”. Journal of Internet Services and Applications, 2 (2). pp. 81-94.

IOSUP A., PRODAN R., and EPEMA D.. IaaS cloud benchmarking: approaches, challenges, and experience. Proc. of IEEE/ACM SC’12, MTAGS

ISO/IEC 27001:2013, Information Security Management System. [Online]. Available: http://www.iso.org.

ISO/IEC 27002:2013, Code of Practice for Information Security Management. [Online]. Available: http://www.iso.org.

ISO/IEC 27005:2011, Information Security Risk Management. [Online]. Available: http://www.iso.org.

KHOSRAVANI, A.; NICHOLSON, B.; WOOD-HARPER, T., “A case study analysis of risk, trust and control in cloud computing”, Science and Information Conference (SAI), 2013, Publication Year: 2013, Page(s): 879- 887.

KOLLURU, N.V.S. ; MANTHA, N. “Cloud integration — Strategy to connect applications to cloud”. India Conference (INDICON), 2013 Annual IEEE. Publication Year: 2013 , Page(s): 1-6.

LENKALA, S.R.; SHETTY, S.; KAIQI XIONG. “Security Risk Assessment of Cloud Carrier”. Cluster, Cloud and Grid Computing (CCGrid), 2013 13th IEEE/ACM International Symposium on, Digital Object Identifier: 10.1109/CCGrid.2013.28, Publication Year: 2013, Page(s): 442- 449.

LIU, S; WU, J.; LU, Z.; XIONG, H., “VMRaS: A Novel Virtual Machine Risk Assessment Scheme in the Cloud Environment”, Services Computing (SCC), 2013 IEEE International Conference on, Digital Object Identifier: 10.1109/SCC.2013.12, Publication Year: 2013, Page(s): 384- 391.

LOR, S., VAQUERO, L.M. ; AUDSIN, D. ; MURRAY, P. “Scalable network-aware data centre federation”. Networks (ICON), 2012 18th IEEE International Conference on. Publication Year: 2012, Page(s): 167- 172.

LUNA, Jesus; LANGENBERG, Robert; SURI, Neeraj. “Benchmarking cloud security level agreements using quantitative policy trees”. Proceeding CCSW '12 Proceedings of the 2012 ACM Workshop on Cloud computing security workshop. Pages 103-112.

MADRIA, S.; SEN, A., "Offline Risk Assessment of Cloud Service Providers," Cloud Computing, IEEE , vol.2, no.3, pp.50,57, May-June 2015. doi: 10.1109/MCC.2015.63.

MELL, P.; GRANCE, T.. “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145 (draft), Jan. 2011, pp. 1–7.

MIRKOVIÉ, O., “Security evaluation in cloud”, Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on, Publication Year: 2013 , Page(s): 1088-1093.

MORIN, J.; AUBERT and B. GATEAU, "Towards Cloud Computing SLA Risk Management: Issues and Challenges," System Science (HICSS), 2012 45th Hawaii International Conference on , vol., no., pp.5509-5514, 4-7 Jan. 2012 doi: 10.1109/HICSS.2012.602.

NIST - National Institute of Standards and Technology, “Guide for Conducting Risk Assessments - Information Security”, Special Publication 800-30 Revision 1, September 2012.

REN, K.; WANG, C.; WANG, Q., "Security Challenges for the Public Cloud," Internet Computing, IEEE, vol.16, no.1, pp.69, 73, Jan.-Feb. 2012 doi: 10.1109/MIC.2012.14.

RISTOV, S., GUSEV, M.; KOSTOSKA, M., "A new methodology for security evaluation in cloud computing," MIPRO, 2012 Proceedings of the 35th International Convention , vol., no., pp.1484-1489, 21-25 May 2012.

RISTOV, S.; GUSEV, M.. “Security evaluation of open source clouds”, EUROCON, 2013 IEEE, Digital Object Identifier: 10.1109/EUROCON. 2013.6624968, Publication Year: 2013, Page(s): 73- 80.

ROT, A.; SOBINSKA, M., “IT security threats in cloud computing sourcing model”, Computer Science and Information Systems (FedCSIS), 2013, Federated Conference on, Publication Year: 2013, Page(s): 1153 - 1156.

SILVA, P. F.; WESTPHALL, C. B. WESTPHALL, C. M., MATTOS, M., SANTOS, D. R. “An Architecture for Risk Analysis in Cloud”. The Tenth International Conference on Networking and Services. InfoSys 2014. ICNS 2014.Charmonix, France. 2014.

SILVA, P. F.; WESTPHALL, C. B. WESTPHALL, C. M., MATTOS, M.. “Model for Cloud Computing Risk Analysis”. The Fourteenth International Conference on Networks. ICN 2015. Barcelona, Espanha. 2015.

SONG, D., “Cloud Data Protection for the Masses”, *Computer*, IEEE, vol.45, no.1, pp.39,45, Jan. 2012 doi: 10.1109/ MC.2012.1

SRINIVASAN, M. K., SARUKESE, K., RODRIGUES, P., MANOJ, M. S., REVATHY, P. “State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment”. ICACCI '12: Proceedings of the International Conference on Advances in Computing, Communications and Informatics. August 2012.

ULLAH, Kazi Wali ; AHMED, Abu Shohel ; YLITALO, Jukka. “Towards Building an Automated Security Compliance Tool for the Cloud”. Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on. Digital Object Identifier: 0.1109/TrustCom. 2013.195. Publication Year: 2013 , Page(s): 1587- 1593.

WANG, P., LIN, W., KOU, S. U., “Threat risk analysis for cloud security based on Attack-Defense Trees”, Computing Technology and Information Management (ICCM), 2012 8th International Conference on, vol.1, no., pp.106-111, 24-26 April 2012.

YU, H., POWELL, N., YUAN, X., “Cloud computing and security challenges”. ACM-SE '12: Proceedings of the 50th Annual Southeast Regional Conference. March 2012.

ZECH, P.; FELDERER , M.; BREU, R., “Towards a Model Based Security Testing Approach of Cloud Computing Environments”, Software Security and Reliability Companion (SERE-C), 2012 IEEE Sixth International Conference on , vol., no., pp.47,56, 20-22 June 2012 doi: 10.1109/SERE-C.2012.11.

ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf. (2010) “Cloud computing: state-of-the-art and research challenges”. Journal of Internet Services and Applications Volume 1, Number 1, 7-18.

ZHANG, J., D. SUN and D. ZHAI, "A research on the indicator system of Cloud Computing Security Risk Assessment," Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), 2012 International

Conference on , vol., no., pp.121,123, 15-18 June 2012 doi: 10.1109/ ICQR2MSE. 2012.6246200.

ZHOU, J.; LI, Shanping; Zhen Zhang; Zhen Ye Zhejiang, “Position paper: cloud-based performance testing: issues and challenges”. Proceeding HotTopiCS '13. Proceedings of the 2013 international workshop on Hot topics in cloud services. Pages 55-62.

APÊNDICE A – CONFIGURAÇÃO DOS WEB SERVICES

A.1. Geração dos Web Services da Conn Layer do RACloud.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"

cls
cd RACloud-Prototype
cd src
apt RACloud\connLayer\ConnCSP.java
pause
apt RACloud\connLayer\ConnCC.java
pause
apt RACloud\connLayer\ConnISL.java
pause
cd..
cd..
cls
```

A.2. Importação dos Web Services nos agentes CC, CSP, ISL.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"

cls
cd RACloud-Prototype
cd bin
start java -classpath . RACloud.RACloudmain
cd..
cd..
pause

cls
cd RACloud-CSP-Agent
cd src
wsimport -keep -p connCSP http://localhost:8080/connCSP?wsdl
pause

cd..
cd..
cd RACloud-ISL-Agent
cd src
wsimport -keep -p connISL http://localhost:8080/connISL?wsdl
pause

cd..
cd..
cd RACloud-CC-Agent
cd src
wsimport -keep -p connCC http://localhost:8080/connCC?wsdl
pause
cd..
cd..
cls
```

A.3. Geração dos Web Services dos Agentes CC, CSP e ISL.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"

cls

cd RACloud-CSP-Agent
cd src
apt CSP_Agent\CSPAgent.java

cd..
cd..
cd RACloud-ISL-Agent
cd src
apt ISL_Agent\ISLAgent.java

cd..
cd..
cd RACloud-CC-Agent
cd src
apt CC_Agent\CCAgent.java
pause
cd..
cd..
cls
```

A.4. Importação dos Web Services dos Agentes no RACloud-Prototype.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"

cls
echo ****** ISL AGENT *********
cd RACloud-ISL-Agent
cd bin
start java ISL_Agent.ISLAgent doNothing
cd..
cd..
pause
cls

echo ****** CSP AGENT *********
cd RACloud-CSP-Agent
cd bin
start java CSP_Agent.CSPAgent doNothing
cd..
cd..
pause
cls

echo ****** CC CONSOLE\AGENT *********
cd RACloud-CC-Agent
cd bin
start java CC_Agent.CCconsole doNothing
cd..
cd..
pause
cls
```

```
echo ****** IMPORTACAO DOS WSs *********
cd RACloud-Prototype
cd src
wsimport -keep -p CSPAgent http://localhost:8081/CSP-DEMO?wsdl
pause

wsimport -keep -p ISLAgent http://localhost:8082/UFSC-LRG-ISL?wsdl

pause

wsimport -keep -p CCAgent  http://localhost:8083/CC-DEMO?wsdl
pause

cd..
cd..
```

A.5. Geração do Web Service de base do CSP-WSRA-Proxy.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"


cd RACloud-CSP-WSRA-Proxy
cd src
apt CSP_WSRA_Proxy\csp_wsra_proxy_base.java

pause
cd..
cd..
cls
```

A.6. Importação do Web Service de base do CSP-WSRA-Proxy para o CSP-Agent.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"

echo ****** CSP WSRA Proxy *********
cd RACloud-CSP-WSRA-Proxy
cd bin
start java CSP_WSRA_Proxy.csp_wsra_proxy_main doNothing
cd..
cd..
pause
cls

cls
cd RACloud-CSP-Agent
cd src
wsimport -keep -p CSP_WSRA_Proxy

http://localhost:8095/csp_wsra_proxy_base?wsdl
pause
cd..
cd..
cls
```

A.7. Geração dos Web Services de análise do ISL-WSRA-Evaluator.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"

cls

cd RACloud-ISL-WSRA-Evaluator
cd src
apt ISL_WSRA_Evaluator\isl9593.java
apt ISL_WSRA_Evaluator\isl0140.java
apt ISL_WSRA_Evaluator\isl1609.java
apt ISL_WSRA_Evaluator\isl3367.java
apt ISL_WSRA_Evaluator\isl0640.java
apt ISL_WSRA_Evaluator\isl0412.java
apt ISL_WSRA_Evaluator\isl2576.java

apt ISL_WSRA_Evaluator\isl459.java
apt ISL_WSRA_Evaluator\isl423.java
apt ISL_WSRA_Evaluator\isl445.java
apt ISL_WSRA_Evaluator\isl254.java
apt ISL_WSRA_Evaluator\isl656.java
apt ISL_WSRA_Evaluator\isl443.java

pause
cd..
cd..
cls
```

A.8. Importação dos WSRAs de análise do ISL-WSRA-Evaluator para o CSP-WSRA-Proxy.

```
set path=%path%;"C:\Program Files\Java\jdk1.7.0_79\bin"

echo ****** ISL WSRA Evaluator *********
cd RACloud-ISL-WSRA-Evaluator
cd bin
start java ISL_WSRA_Evaluator.isl_wsra_evaluator_main
cd..
cd..
pause
cls

cd RACloud-CSP-WSRA-Proxy
cd src

wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl9593?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl0140?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl1609?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl3367?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl0640?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl0412?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl2576?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl7203?wsdl

wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl459?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl423?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl445?wsdl
```

```
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl254?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl656?wsdl
wsimport -keep -p ISL_WSRA_Evaluator http://localhost:8091/isl443?wsdl

pause
cd..
cd..
cls
```

APÊNDICE B – EXECUÇÃO DO MODELO RACLOUD

B.1. Execução da entidade RAP.

```
cls
echo ****** RACLOUD *********
cd RACloud-Prototype
cd bin
start java RACloud.RACloudmain doRiskAnalysis
cd..
cd..
pause
cls
```

B.2. Execução da entidade ISL.

```
echo ****** ISL-GENT *********
cd RACloud-ISL-Agent
cd bin
start java ISL_Agent.ISLAgent doRiskAnalysis
cd..
cd..
pause
cls

echo ****** ISL-WSRA-Evaluator *********
cd RACloud-ISL-WSRA-Evaluator
cd bin
start java ISL_WSRA_Evaluator.isl_wsra_evaluator_main doRiskAnalysis
cd..
cd..
pause
cls
```

B.3. Execução da entidade CSP.

```
echo ****** CSP-AGENT *********
cd RACloud-CSP-Agent
cd bin
start java CSP_Agent.CSPAgent doRiskAnalysis
cd..
cd..
pause
cls

echo ****** CSP-WSRA-Proxy *********
cd RACloud-CSP-WSRA-Proxy
cd bin
start java CSP_WSRA_Proxy.csp_wsra_proxy_main doRiskAnalysis
cd..
cd..
pause
cls
```

B.4. Execução da entidade CC.

```
echo ****** CC CONSOLE\AGENT *********
cd RACloud-CC-Agent
cd bin
java CC_Agent.CCconsole doRiskAnalysis
```

APÊNDICE C – CONFIGURAÇÃO DOS AGENTES

C.1. Arquivo de configuração do CC-Agent (cc.conf).

```
name = CC-DEMO
csp_target = CSP-DEMO
port = 8083
rdl_path = C:/Raíz Web/Dropbox/Diversos/workspace-java/RACloud-CC-
Agent/rdl_database/
risk_path = C:/Raíz Web/Dropbox/Diversos/workspace-java/RACloud-CC-
Agent/risk_database/
```

C.2. Arquivo de configuração do Agente CSP (csp.conf).

```
name = CSP-DEMO
port = 8081

subscribers = UFSC-LRG-ISL@1299,UFSC-LRG-ISL@8796

isl9593 = http://localhost:8095/csp9593
isl0140 = http://localhost:8095/csp0140
isl1609 = http://localhost:8095/csp1609
isl3367 = http://localhost:8095/csp3367
isl0640 = http://localhost:8095/csp0640
isl0412 = http://localhost:8095/csp0412
isl2576 = http://localhost:8095/csp2576
isl7203 = http://localhost:8095/csp7203

isl459 = http://localhost:8095/csp459
isl423 = http://localhost:8095/csp423
isl445 = http://localhost:8095/csp445
isl254 = http://localhost:8095/csp254
isl656 = http://localhost:8095/csp656
isl443 = http://localhost:8095/csp443
```

C.3. Arquivo de configuração do Agente ISL (isl.conf).

```
name = UFSC-LRG-ISL
port = 8082
rdl_path = C:/Raíz Web/Dropbox/Diversos/workspace-java/RACloud-ISL-
Agent/rdl_database/
```

APÊNDICE D – RDLs DOS AGENTES CC E ISL

D.1. RDL de definição de ativos de informação do Agente CC (rdl_asset.xml).

```
<?xml version="1.0" ?>
<RDL type="CC" id="5699">
          <source>Consumer-X</source>
          <version>4.5.1a</version>
          <description>...</description>
          <informationAssets>
                    <item id="001">
                              <description>Contratos de clientes</description>
                              <category>File</category>
                              <confidenciality>75</confidenciality>
                              <integrity>80</integrity>
                              <availability>68</availability>
                    </item>
                    <item id="002">
                              <description>Informacoes financeiras</description>
                              <category>Database</category>
                              <confidenciality>80</confidenciality>
                              <integrity>90</integrity>
                              <availability>60</availability>
                    </item>
                    <item id="003">
                              <description>Sistema de Pedidos</description>
                              <category>CC-Software</category>
                              <resources>
                                        <resource>Database</resource>
                                        <resource>Framework</resource>
                                        <resource>Application Server</resource>
                              </resources>
                              <confidenciality>60</confidenciality>
                              <integrity>85</integrity>
                              <availability>80</availability>
                    </item>
                    <item id="004">
                              <description>Sistema help desk</description>
                              <category>CSP-Software</category>
                              <resources>
                                        <resource>Framework</resource>
                                        <resource>Application Server</resource>
                              </resources>
                              <confidenciality>40</confidenciality>
                              <integrity>70</integrity>
                              <availability>85</availability>
                    </item>
          </informationAssets>
</RDL>
```

D.2. RDL de definição de vulnerabilidades no Agente ISL (rdl_vuln.xml).

```
<?xml version="1.0" ?>
<RDL type="ISL" id="1299">
          <source>LRG-UFSC</source>
          <version>1.3</version>
          <description>...</description>
          <vulnerabilities>
        <item id="9593" propertyC="true" propertyI="true" propertyA="false">
            <description>Apache CloudStack before 4.3.2 allow obtain private
key</description>
            <category>Communication System</category>
            <wsra>http://localhost:8095/isl9593</wsra>
            <reference>CVE-2014-9593</reference>
        </item>
        <item id="0140" propertyC="true" propertyI="true" propertyA="true">
```

```
            <description>Red Hat CloudForms 3.1 allow Unauthorised
actions</description>
            <category>Cloud System</category>
            <wsra>http://localhost:8095/isl0140</wsra>
            <reference>CVE-2014-0140</reference>
        </item>
        <item id="1609" propertyC="false" propertyI="false" propertyA="true">
            <description>MongoDB before 2.4.13 allows denial of service</description>
            <category>Database</category>
            <wsra>http://localhost:8095/isl1609</wsra>
            <reference>CVE-2015-1609</reference>
        </item>
        <item id="3367" propertyC="true" propertyI="true" propertyA="true">
            <description>Cross-site scripting (XSS) vulnerability in the vCloud
VMWare</description>
            <category>VM System</category>
            <wsra>http://localhost:8095/isl3367</wsra>
            <reference>CVE-2014-3367</reference>
        </item>
        <item id="0640" propertyC="false" propertyI="false" propertyA="true">
            <description>HSL feature in Cisco IOS XE 2.x Dos via IP</description>
            <category>Communication System</category>
            <wsra>http://localhost:8095/isl0640</wsra>
            <reference>CVE-2015-0640</reference>
        </item>
        <item id="0412" propertyC="true" propertyI="true" propertyA="true">
            <description>Oracle Java SE 6u85 vulnerability related to JAX-
WS</description>
            <category>Framework</category>
            <wsra>http://localhost:8095/isl0412</wsra>
            <reference>CVE-2015-0412</reference>
        </item>
        <item id="2576" propertyC="false" propertyI="true" propertyA="false">
            <description>MySQL 1.5.1 and earlier integrity failure</description>
            <category>Database</category>
            <wsra>http://localhost:8095/isl2576</wsra>
            <reference>CVE-2015-2576</reference>
        </item>
     </vulnerabilities>
</RDL>
```

D.3. RDL de definição de ameaças no Agente ISL (rdl_treats.xml).

```
<?xml version="1.0" ?>
<RDL type="ISL" id="8796">
          <source>LRG-UFSC</source>
          <version>1.3</version>
          <description>...</description>
    <threats>
        <item id="459" propertyC="true" propertyI="false" propertyA="false">
            <description>Remote spying</description>
            <type>Compromise of information</type>
            <category>Communication System</category>
            <wsra>http://localhost:8091/isl459</wsra>
            <reference>ISO 27005</reference>
        </item>
        <item id="423" propertyC="false" propertyI="false" propertyA="true">
            <description>Saturation of the system</description>
            <type>Technical failures</type>
            <category>Cloud System</category>
            <wsra>http://localhost:8091/isl423</wsra>
            <reference>ISO 27005</reference>
        </item>
        <item id="445" propertyC="false" propertyI="true" propertyA="false">
            <description>Corruption of data</description>
            <type>Unauthorised actions</type>
            <category>Database</category>
            <wsra>http://localhost:8091/isl445</wsra>
            <reference>ISO 27005</reference>
        </item>
```

```
        <item id="254" propertyC="true" propertyI="true" propertyA="true">
            <description>Inter-VM violation</description>
            <type>Unauthorised actions</type>
            <category>VM System</category>
            <wsra>http://localhost:8091/isl254</wsra>
            <reference>CSA Guide</reference>
        </item>
        <item id="656" propertyC="true" propertyI="true" propertyA="false">
            <description>Tampering on transit</description>
            <type>Compromise of information</type>
            <category>Communication System</category>
            <wsra>http://localhost:8091/isl656</wsra>
            <reference>CSA Guide</reference>
        </item>
        <item id="443" propertyC="true" propertyI="true" propertyA="true">
            <description>Spoofing of user</description>
            <type>Compromise of functions</type>
            <category>Framework</category>
            <wsra>http://localhost:8091/isl443</wsra>
            <reference>CSA Guide</reference>
        </item>
    </threats>
</RDL>
```

APÊNDICE E – RDL DE RISCO RESULTANTE

RDL de risco resultante após utilização do protótipo (rdl_risk.xml).

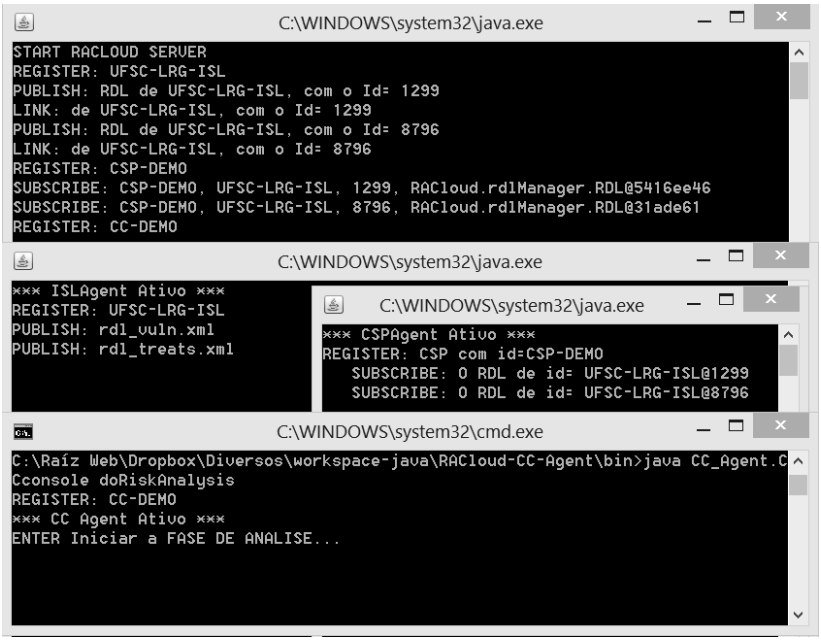
```
<?xml version="1.0" encoding="UTF-8"?>
<RDL Id="248" type="RISK">
   <source>RACloud-LRG</source>
   <version>5a</version>
   <description>...</description>
   <cc_id>consumerCC</cc_id>
   <csp_id>amazonCSP</csp_id>
   <risks>
      <risk_item DRa="0" DRc="72" DRi="0" id="1">
         <informationAsset DIa="68" DIc="75" DIi="80" id="001">Contratos de
clientes</informationAsset>
         <event Pa="0" Pc="70" Pi="0" id="9593@459">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="0" id="459">Remote spying</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="72" DRi="67" id="2">
         <informationAsset DIa="68" DIc="75" DIi="80" id="001">Contratos de
clientes</informationAsset>
         <event Pa="0" Pc="70" Pi="55" id="9593@656">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="60" id="656">Tampering on transit</threat>
         </event>
      </risk_item>
      <risk_item DRa="71" DRc="0" DRi="0" id="3">
         <informationAsset DIa="68" DIc="75" DIi="80" id="001">Contratos de
clientes</informationAsset>
         <event Pa="75" Pc="0" Pi="0" id="0140@423">
            <vulnerability DDa="70" DDc="90" DDi="80" id="0140">Red Hat CloudForms
3.1 allow Unauthorised actions</vulnerability>
            <threat DEa="80" DEc="0" DEi="0" id="423">Saturation of the
system</threat>
         </event>
      </risk_item>
      <risk_item DRa="49" DRc="77" DRi="62" id="4">
         <informationAsset DIa="68" DIc="75" DIi="80" id="001">Contratos de
clientes</informationAsset>
         <event Pa="30" Pc="80" Pi="45" id="3367@254">
            <vulnerability DDa="30" DDc="70" DDi="50" id="3367">Cross-site scripting
(XSS) vulnerability in the vCloud VMWare</vulnerability>
            <threat DEa="30" DEc="90" DEi="40" id="254">Inter-VM violation</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="75" DRi="0" id="5">
         <informationAsset DIa="60" DIc="80" DIi="90" id="002">Informacoes
financeiras</informationAsset>
         <event Pa="0" Pc="70" Pi="0" id="9593@459">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="0" id="459">Remote spying</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="75" DRi="72" id="6">
         <informationAsset DIa="60" DIc="80" DIi="90" id="002">Informacoes
financeiras</informationAsset>
         <event Pa="0" Pc="70" Pi="55" id="9593@656">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="60" id="656">Tampering on transit</threat>
         </event>
      </risk_item>
      <risk_item DRa="67" DRc="0" DRi="0" id="7">
         <informationAsset DIa="60" DIc="80" DIi="90" id="002">Informacoes
financeiras</informationAsset>
```

```
         <event Pa="75" Pc="0" Pi="0" id="0140@423">
            <vulnerability DDa="70" DDc="90" DDi="80" id="0140">Red Hat CloudForms
3.1 allow Unauthorised actions</vulnerability>
            <threat DEa="80" DEc="0" DEi="0" id="423">Saturation of the
system</threat>
         </event>
      </risk_item>
      <risk_item DRa="45" DRc="80" DRi="67" id="8">
         <informationAsset DIa="60" DIc="80" DIi="90" id="002">Informacoes
financeiras</informationAsset>
         <event Pa="30" Pc="80" Pi="45" id="3367@254">
            <vulnerability DDa="30" DDc="70" DDi="50" id="3367">Cross-site scripting
(XSS) vulnerability in the vCloud VMWare</vulnerability>
            <threat DEa="30" DEc="90" DEi="40" id="254">Inter-VM violation</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="0" DRi="81" id="9">
         <informationAsset DIa="60" DIc="80" DIi="90" id="002">Informacoes
financeiras</informationAsset>
         <event Pa="0" Pc="0" Pi="72" id="2576@445">
            <vulnerability DDa="0" DDc="0" DDi="55" id="2576">MySQL 1.5.1 and earlier
integrity failure</vulnerability>
            <threat DEa="0" DEc="0" DEi="90" id="445">Corruption of data</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="65" DRi="0" id="10">
         <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de
Pedidos</informationAsset>
         <event Pa="0" Pc="70" Pi="0" id="9593@459">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="0" id="459">Remote spying</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="65" DRi="70" id="11">
         <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de
Pedidos</informationAsset>
         <event Pa="0" Pc="70" Pi="55" id="9593@656">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="60" id="656">Tampering on transit</threat>
         </event>
      </risk_item>
      <risk_item DRa="77" DRc="0" DRi="0" id="12">
         <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de
Pedidos</informationAsset>
         <event Pa="75" Pc="0" Pi="0" id="0140@423">
            <vulnerability DDa="70" DDc="90" DDi="80" id="0140">Red Hat CloudForms
3.1 allow Unauthorised actions</vulnerability>
            <threat DEa="80" DEc="0" DEi="0" id="423">Saturation of the
system</threat>
         </event>
      </risk_item>
      <risk_item DRa="55" DRc="70" DRi="65" id="13">
         <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de
Pedidos</informationAsset>
         <event Pa="30" Pc="80" Pi="45" id="3367@254">
            <vulnerability DDa="30" DDc="70" DDi="50" id="3367">Cross-site scripting
(XSS) vulnerability in the vCloud VMWare</vulnerability>
            <threat DEa="30" DEc="90" DEi="40" id="254">Inter-VM violation</threat>
         </event>
      </risk_item>
      <risk_item DRa="77" DRc="62" DRi="72" id="14">
         <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de
Pedidos</informationAsset>
         <event Pa="75" Pc="65" Pi="60" id="0412@443">
            <vulnerability DDa="90" DDc="40" DDi="30" id="0412">Oracle Java SE 6u85
vulnerability related to JAX-WS</vulnerability>
            <threat DEa="60" DEc="90" DEi="90" id="443">Spoofing of user</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="0" DRi="78" id="15">
```

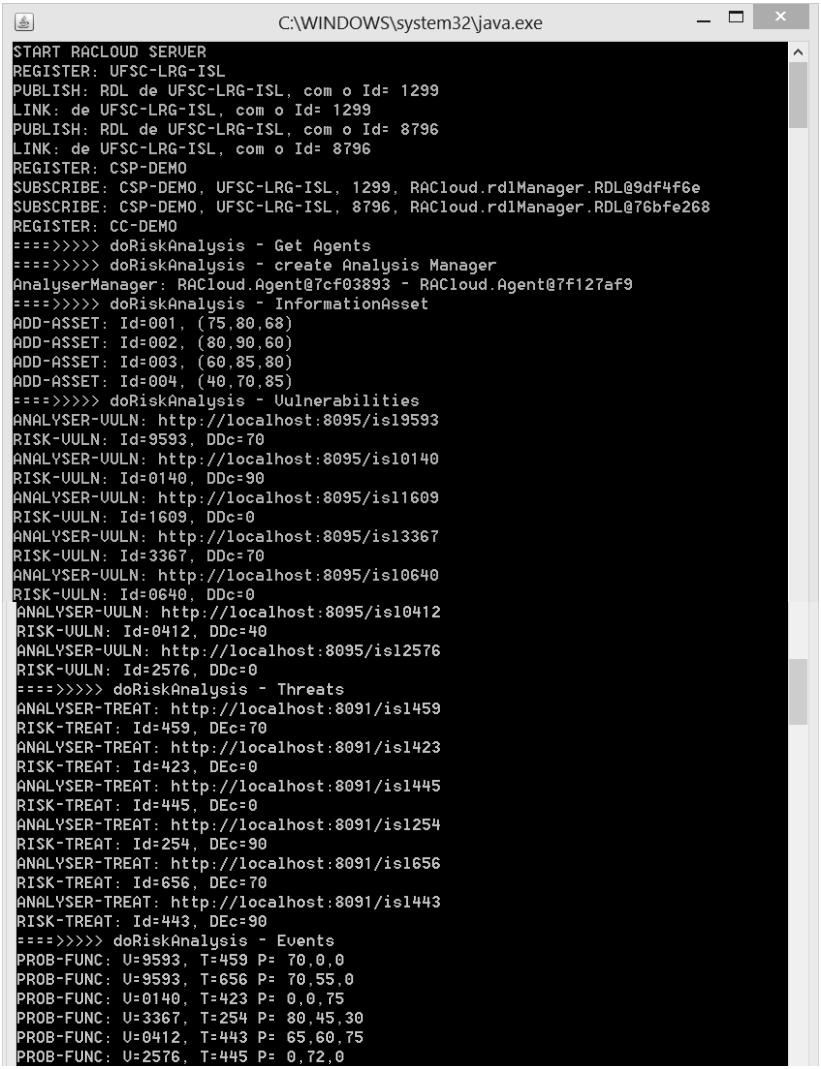
```
         <informationAsset DIa="80" DIc="60" DIi="85" id="003">Sistema de
Pedidos</informationAsset>
         <event Pa="0" Pc="0" Pi="72" id="2576@445">
            <vulnerability DDa="0" DDc="0" DDi="55" id="2576">MySQL 1.5.1 and earlier
integrity failure</vulnerability>
            <threat DEa="0" DEc="0" DEi="90" id="445">Corruption of data</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="55" DRi="0" id="16">
         <informationAsset DIa="85" DIc="40" DIi="70" id="004">Sistema help
desk</informationAsset>
         <event Pa="0" Pc="70" Pi="0" id="9593@459">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="0" id="459">Remote spying</threat>
         </event>
      </risk_item>
      <risk_item DRa="0" DRc="55" DRi="62" id="17">
         <informationAsset DIa="85" DIc="40" DIi="70" id="004">Sistema help
desk</informationAsset>
         <event Pa="0" Pc="70" Pi="55" id="9593@656">
            <vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack
before 4.3.2 allow obtain private key</vulnerability>
            <threat DEa="0" DEc="70" DEi="60" id="656">Tampering on transit</threat>
         </event>
      </risk_item>
      <risk_item DRa="80" DRc="0" DRi="0" id="18">
         <informationAsset DIa="85" DIc="40" DIi="70" id="004">Sistema help
desk</informationAsset>
         <event Pa="75" Pc="0" Pi="0" id="0140@423">
            <vulnerability DDa="70" DDc="90" DDi="80" id="0140">Red Hat CloudForms
3.1 allow Unauthorised actions</vulnerability>
            <threat DEa="80" DEc="0" DEi="0" id="423">Saturation of the
system</threat>
         </event>
      </risk_item>
      <risk_item DRa="57" DRc="60" DRi="57" id="19">
         <informationAsset DIa="85" DIc="40" DIi="70" id="004">Sistema help
desk</informationAsset>
         <event Pa="30" Pc="80" Pi="45" id="3367@254">
            <vulnerability DDa="30" DDc="70" DDi="50" id="3367">Cross-site scripting
(XSS) vulnerability in the vCloud VMWare</vulnerability>
            <threat DEa="30" DEc="90" DEi="40" id="254">Inter-VM violation</threat>
         </event>
      </risk_item>
      <risk_item DRa="80" DRc="52" DRi="65" id="20">
         <informationAsset DIa="85" DIc="40" DIi="70" id="004">Sistema help
desk</informationAsset>
         <event Pa="75" Pc="65" Pi="60" id="0412@443">
            <vulnerability DDa="90" DDc="40" DDi="30" id="0412">Oracle Java SE 6u85
vulnerability related to JAX-WS</vulnerability>
            <threat DEa="60" DEc="90" DEi="90" id="443">Spoofing of user</threat>
         </event>
      </risk_item>
   </risks>
</RDL>
```

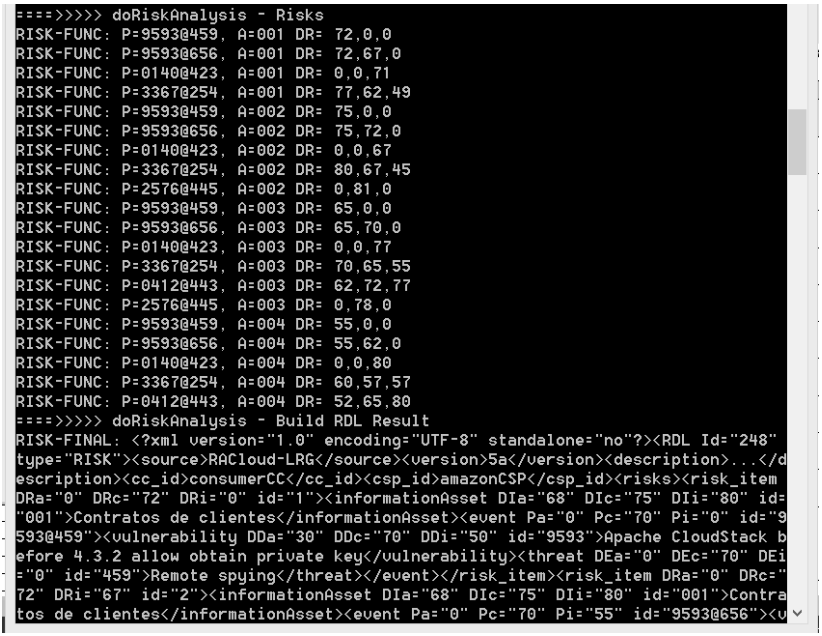
APÊNDICE F – LOGS DE EXECUÇÃO DO PROTÓTIPO

F.1 Log de execução das entidades na fase de especificação do risco.

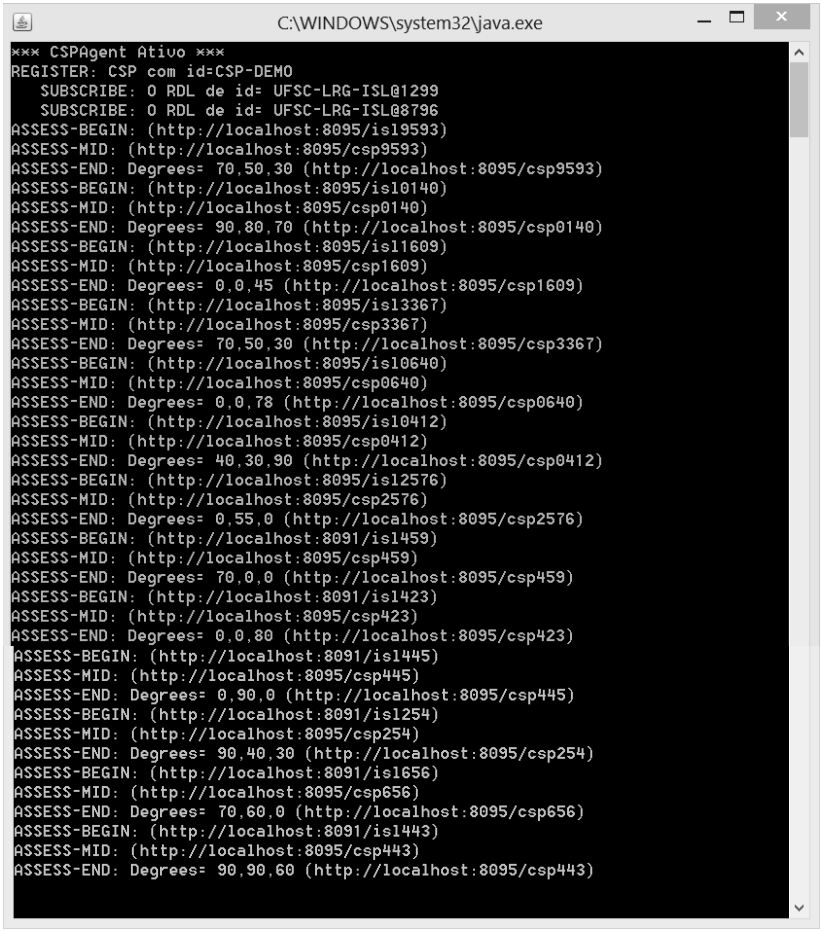


F.2 Log de execução do projeto RACloud-Prototype.

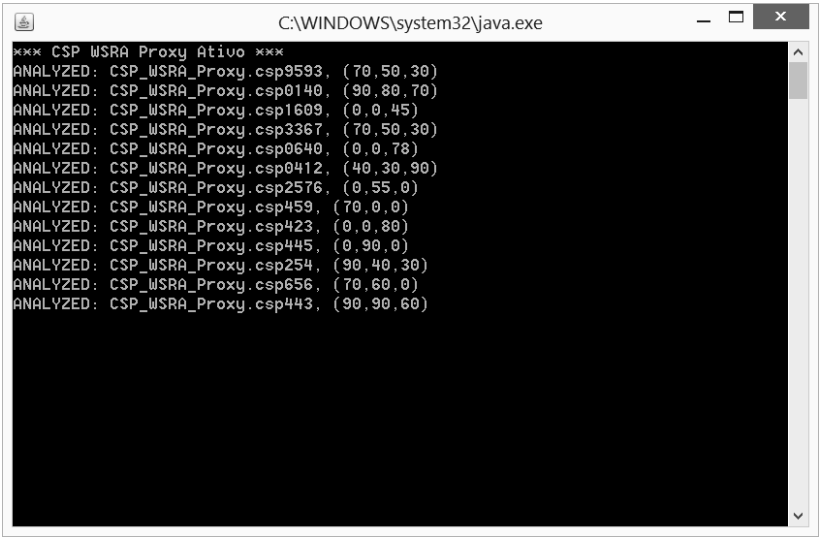



====>>>>> doRiskAnalysis - Risks
RISK-FUNC: P=9593@459, A=001 DR= 72,0,0
RISK-FUNC: P=9593@656, A=001 DR= 72,67,0
RISK-FUNC: P=0140@423, A=001 DR= 0,0,71
RISK-FUNC: P=3367@254, A=001 DR= 77,62,49
RISK-FUNC: P=9593@459, A=002 DR= 75,0,0
RISK-FUNC: P=9593@656, A=002 DR= 75,72,0
RISK-FUNC: P=0140@423, A=002 DR= 0,0,67
RISK-FUNC: P=3367@254, A=002 DR= 80,67,45
RISK-FUNC: P=2576@445, A=002 DR= 0,81,0
RISK-FUNC: P=9593@459, A=003 DR= 65,0,0
RISK-FUNC: P=9593@656, A=003 DR= 65,70,0
RISK-FUNC: P=0140@423, A=003 DR= 0,0,77
RISK-FUNC: P=3367@254, A=003 DR= 70,65,55
RISK-FUNC: P=0412@443, A=003 DR= 62,72,77
RISK-FUNC: P=2576@445, A=003 DR= 0,78,0
RISK-FUNC: P=9593@459, A=004 DR= 55,0,0
RISK-FUNC: P=9593@656, A=004 DR= 55,62,0
RISK-FUNC: P=0140@423, A=004 DR= 0,0,80
RISK-FUNC: P=3367@254, A=004 DR= 60,57,57
RISK-FUNC: P=0412@443, A=004 DR= 52,65,80
====>>>>> doRiskAnalysis - Build RDL Result
RISK-FINAL: <?xml version="1.0" encoding="UTF-8" standalone="no"?><RDL Id="248"
type="RISK"><source>RACloud-LRG</source><version>5a</version><description>...</d
escription><cc_id>consumerCC</cc_id><csp_id>amazonCSP</csp_id><risks><risk_item
DRa="0" DRc="72" DRi="0" id="1"><informationAsset DIa="68" DIc="75" DIi="80" id=
"001">Contratos de clientes</informationAsset><event Pa="0" Pc="70" Pi="0" id="9
593@459"><vulnerability DDa="30" DDc="70" DDi="50" id="9593">Apache CloudStack b
efore 4.3.2 allow obtain private key</vulnerability><threat DEa="0" DEc="70" DEi
="0" id="459">Remote spying</threat></event></risk_item><risk_item DRa="0" DRc="
72" DRi="67" id="2"><informationAsset DIa="68" DIc="75" DIi="80" id="001">Contra
tos de clientes</informationAsset><event Pa="0" Pc="70" Pi="55" id="9593@656"><v

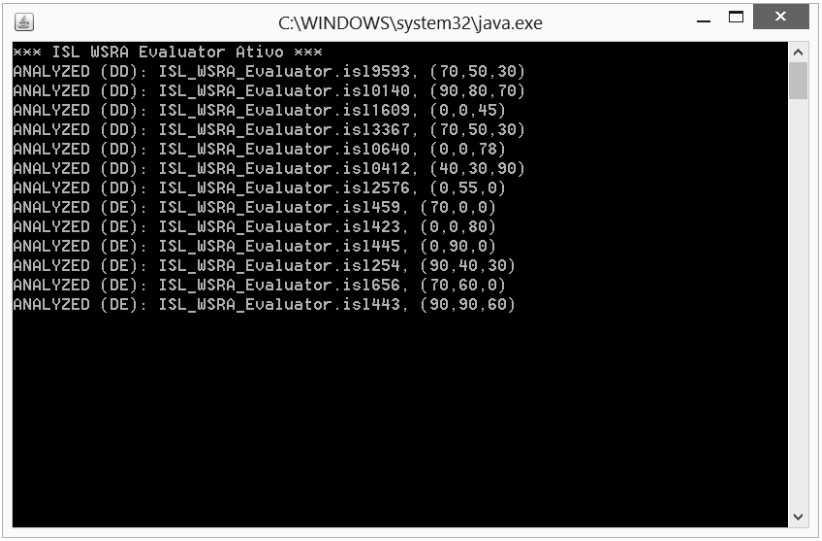
F.3 Logs de execução do projeto RACloud-CSP-Agent.



F.4 Logs de execução do projeto RACloud-CSP-WSRA-Proxy.



F.5 Log de execução do projeto RACloud-ISL-WSRA-Evaluator.



F.6 Log de execução do projeto RACloud-CC-Agent.